Intel® NetStructure™ 7110/7115 e-Commerce Accelerator

Version 2.3

User Guide

A31032-001

Copyright

This User Guide as well as the software described in it is furnished under license and may only be used or copied in accordance with the terms of the license. The information in this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document.

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel® products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

Trademarks

Intel, NetStructure™ 7110 e-Commerce Accelerator, and NetStructure™ 7115 e-Commerce Accelerator are trademarks of or trademarks applied for by Intel Corporation.

§ Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.

Intel Corporation
Network Equipment Division
13280 Evening Creek Drive
San Diego, California 92128-4102
USA

July 28, 2000 **A31032-001**

Table of Contents

Chapter 3: Theory of Operation

Chapter 4: Scenarios

Chapter 5: Command Reference

Chapter 6: Remote Management

Chapter 7: Alarms and Monitoring

Chapter 8: Software Updates

List of Figures

1 Introduction

Congratulations on your choice of the Intel® NetStructure™ 7110/7115 e-Commerce Accelerator. The processing of secure transactions through Secure Socket Layer (SSL) can occupy up to 90% of even the largest servers' CPU power and can degrade response time significantly. The 7110/7115 provides a completely transparent way to increase the performance of Web sites for SSL transactions. The 7110/7115 is positioned in front of the server farm, where it intercepts SSL transactions, processes them, and relays them to the servers. The 7110/7115 performs all encryption and decryption management in this environment with a minimum of administrator interaction.

About this User Guide

This User Guide supports the Intel® NetStructure™ 7110 e-Commerce Accelerator and the Intel® NetStructure™ 7115 e-Commerce Accelerator. By default this text refers to the product as "7110/7115." Where appropriate, the text refers to "7110" or "7115." Additionally, notes in the left-hand margin may be used to distinguish the two products. Illustrations of the command prompt use "`Intel 7115>`."

New in This Release

New features in the Intel® NetStructure™ 7110/7115 e-Commerce Accelerator include:

- **Improved performance**: Threefold increase in SSL connections processed per second—from 200 to 600 *(7115 only)*
- **More certificate mappings**: Up to 1000 certificate mappings supported
- **Remote Management**:
  - Telnet—standard remote access to the Command Line Interface (CLI) with new "Console Monitoring" features
  - SSh—complete, secure CLI access with new "Console Monitoring" features
  - SNMP—Includes both Private Enterprise MIB and MIBII functionality
- **Alarms**: The 7110/7115 can be configured to display—at the administration console or a remote management session (Telnet and SSh)—autonomous one-line reports of the following exceptional conditions:
  - Encryption status change
  - Refused SSL connections
  - Threshold alerts
  - Overload alerts
  - Network link status

- **Monitoring**: Users can now configure the 7110/7115 to send periodic multi-status reports to the administration console or a remote management session (Telnet and SSh). Monitor reports include such information as:
  - Inline/bypass mode
  - Failsafe/failthrough mode
  - CPU status
  - SSL connections status
  - Network interface status
  - Server interface status
  - Rate of encryption/decryption

Who Should Use this Book

This User Guide is intended for administrators with the following background:

- Familiarity with networking concepts and terminology.
- Basic knowledge of network topologies.
- Basic knowledge of networks and IP routing.
- Some knowledge of SSL, keys, and certificates.
- Knowledge of Web servers.

Before You Begin

7110/7115 setup can be divided into three basic procedures:

- Physically install single or multiple 7110/7115s with single or multiple servers.
- Configure your 7110/7115 in the Command Line Interface.
- Identify existing certificates or obtain new ones you wish to use in SSL operations.

How to Use this Book

The information in this book is organized as follows:

- *Chapter 1: Introduction* provides an introduction and overview of the 7110/7115, and a summary of new features.
- *Chapter 2: Installation and Initial Configuration* contains installation and initial configuration procedures. (This material is also discussed in the separate *Quick Start Guide*.)
- *Chapter 3: Theory of Operation* explains the general principles behind 7110/7115 operation.
- *Chapter 4: Scenarios* provides examples of 7110/7115 configurations, together with specific procedures for their implementation.
- *Chapter 5: Command Reference* explains the Command Line Interface (CLI), and lists the commands and their functions.
- *Chapter 6: Remote Management* details how you can use Telnet, Secure Shell (SSH), and SNMP to manage the 7110/7115 from remote locations.
- *Chapter 7: Alarms and Monitoring* explains the ways in which you can configure the device to report information to you, either routinely or as a result of abnormal events or conditions.
- *Chapter 8: Software Updates* provides procedures for obtaining 7110/7115 system software updates.
- *Chapter 9: Troubleshooting* is a table containing symptoms of problems you may encounter with corresponding likely causes and remedies.
- *Appendix A: Front Panel* diagrams and explains the 7110/7115's front panel LEDs, buttons, and connections.
- *Appendix B: Failure/Bypass Modes* explains how the 7110/7115 deals with failure conditions and details the bypass function.
- *Appendix C: Supported Ciphers* lists the supported encryption ciphers.
- *Appendix D: Regulatory Information* provides information regarding the 7110/7115's compliance with applicable regulations.

- *Appendix E: Terms and Conditions* contains the software license and terms and conditions of user of this product.
- *Glossary* defines terms appearing in this User Guide.

Notes

2 Installation and Initial Configuration

Intel® NetStructure™ 7110/7115 e-Commerce Accelerator installation and initial configuration instructions are in this chapter.

Before You Begin

WARNING: *Do not remove the cover. There are no user-servicable parts inside.*

Before you begin installation, you need the following:

- IP address for 7110/7115 (only if you intend to use the Remote Management)
- IP addresses and ports of servers.
- Keys/certificates. See Chapter 3 for information on obtaining keys and certificates.
- Network cables, such as straight-through and/or crossover cables. (Procedures in the section,“Wiring Connections” in this chapter will identify the types of cables you must use.) If you are installing the 7110/7115 in a rack, you will also need:
- Phillips screwdriver
- Rack-mounting screws

Installing the 7110/7115 Free-Standing or in a Rack

The Intel® NetStructure™ 7110/7115 e-Commerce Accelerator is physically installed in either of two ways:

- In a standard 19” rack, cantilevered from the provided mounting brackets
- Free-standing on a flat surface with sufficient space for air-flow

Rack Installation

Rack mounting requires the use of the mounting brackets, and all four of the included Phillips screws.

1. Locate the two mounting brackets and the four screws. (Two screws for each bracket.)
2. Attach a mounting bracket to each side of the 7110/7115, using two of the provided screws for each bracket. Use the holes near the front of the 7110/7115’s sides. The brackets have both round and oval holes; the flange with round holes attaches to the 7110/7115, the oval holes to the rack.

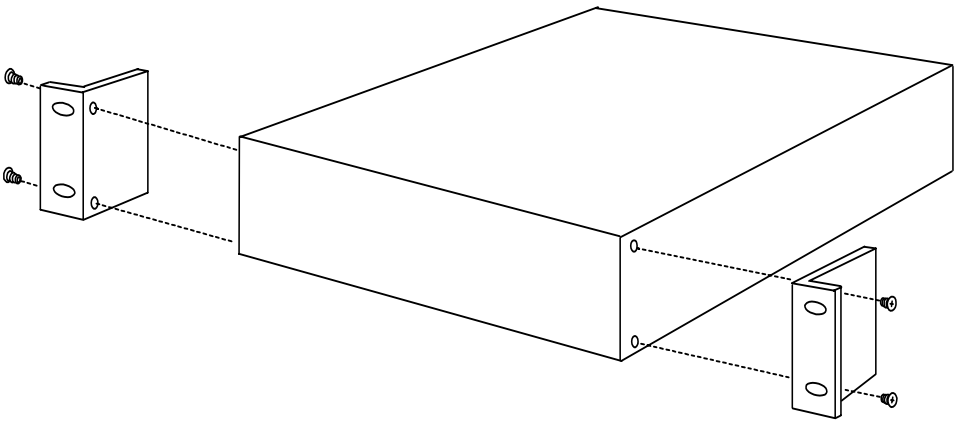

Figure 2-1: Mounting Bracket Orientation

3. Position the 7110/7115 in the desired space of your 19" rack and attach the front flange of each mounting bracket to the rack with two screws each. (Rack-mounting screws are not provided.)

Free-Standing Installation

1. Attach the provided self-adhesive rubber feet to the 7110/7115's bottom.
2. Place the 7110/7115 on a flat surface and make sure that there is adequate airflow surrounding the unit (allow at least one inch of air space on all sides).

Network Connections

1. Use the "Network Cable Requirements" table near the beginning of this guide to select and install the the appropriate cables.

NOTE: *Never connect both ports to the same network segment (e.g., to the same hub or switch). Doing so creates a feedback loop that adversely effects network bandwidth.*

2. Connect the provided power cable to the back of the unit. (There is no power switch.) Under normal circumstances, the 7110/7115 requires approximately 30 seconds to boot. When the boot is complete, the unit's Power LED is steadily illuminated. (If the Power LED is not steadily illuminated, see Chapter 9, "Troubleshooting.)
3. If the Inline LED is neither steadily illuminated or blinking, press the Bypass switch.
4. At this point both the Network and Server LEDs should be steadily illuminated. If not, please see Chapter 9, "Troubleshooting.

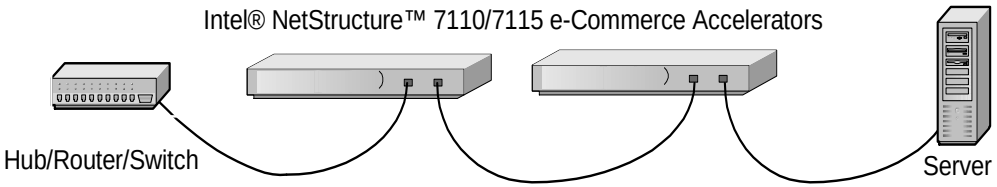

Figure 2-2: Wiring Connections

Status Check

Before proceeding to the PC Initialization section, take a moment to verify that the 7110/7115 is correctly connected.

Network and Server LEDs

Verify that the Network and Server LEDs are both illuminated. If one or both are not, refer to the Troubleshooting section at the end of this chapter.

Inline LED

A blinking Inline LED indicates that the system is online in Fail-safe mode. Refer the Troubleshooting section at the end of this chapter or Appendix B, “Failure/Bypass Modes.”

Admin Terminal Connection

Run HyperTerminal§ or a similar terminal emulator on your PC. The steps below are illustrative of HyperTerminal§. Other terminals will require different procedures.

1. Use the serial cable provided with the 7110/7115 to connect the device’s serial port (the left-hand serial port labeled “Console”) to the serial port of any terminal. (A PC running Windows HyperTerminal§ is used here as an example.)

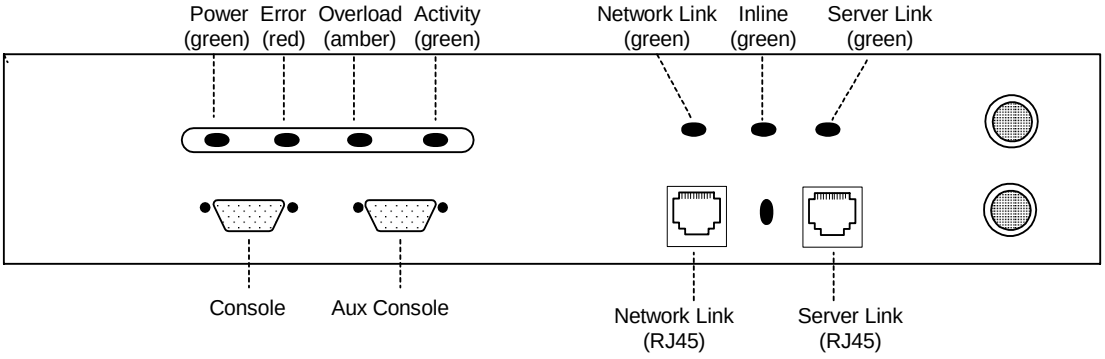

Figure 2-3: Front Panel Connectors and LEDs

2. Type an appropriate name in the Name field of the Connection Description window (e.g., “Configuration”), and then click the **OK** button. The **Phone Number** panel appears.
3. In the **Connect Using…** field specify “Direct to COM1” (or the serial port through which the PC is connected to the 7110/7115 if different from COM1).
4. Click the **OK** button. The COM1 Properties panel appears. Set the values displayed here to **9600**, **8**, **none**, **1**, and **none**.
5. Click the **OK** button.

HyperTerminal§ Paste Operations

If you’re using Hyperterminal§ you **must** make the following configuration change:

1. In the **File** menu, click **Properties**.
2. Click the **Settings** tab.
3. Click the **ASCII Setup** button.
4. Change the values of Line and Character delay from 0 to at least 1 millisecond.
5. Click **OK** twice to exit.

Troubleshooting

Server and Network LEDs

If either the Network or Server LED fails to illuminate using either straight-through or crossover network cables, the problem may be elsewhere in the network. Verify by wiring around the 7110/7115.

Inline LED

The Fail-through switch allows you to control what happens in the event of a failure. It is located in a recess between the Network and Server connectors. Use a small screwdriver or paper clip to manipulate the switch. The two options are:

- Allow traffic to flow through the 7110/7115 unprocessed. (Fail-through mode, indicated by a steadily illuminated Inline LED.)
- Block traffic flow through the 7110/7115 entirely. (Fail-safe mode, indicated by a blinking Inline LED.)

Please see Appendix B for a table describing all permutations of LED operation.

Continuing Configuration

This concludes basic configuration of the 7110/7115. To configure the unit for production please continue with Chapter 3, *Theory of Operations*, or Chapter 4, *Scenarios*.

3 Theory of Operation

Security

New in the Intel® NetStructure™ 7110/7115 e-Commerce Accelerator is Remote Management capability. This feature requires that the 7110/7115's network interface be assigned an IP address, thus security becomes a matter for your attention. If you intend to manage your 7110/7115 from a remote location, be sure to read the section "Access Control," Chapter 6, "Remote Management."

Single Server Acceleration

Typically, the Intel® NetStructure™ 7110/7115 e-Commerce Accelerator supports the SSL processing needs of a single server. This is the simplest and most common configuration. The 7110/7115 is connected to the network between the router and the server.

Ideally, the 7110/7115 is located in the same rack as the server, separated by a short distance. .

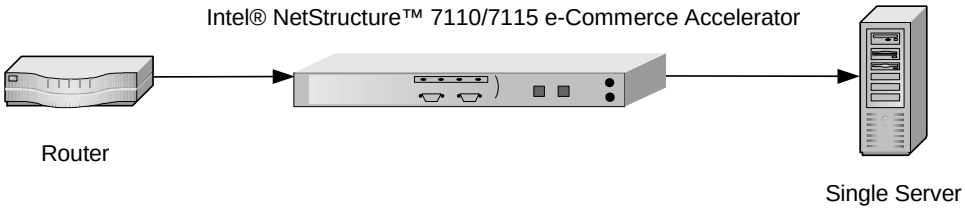

Figure 3-1: 7110/7115 in Single Server Configuration

Multiple Servers

Given the SSL processing power of the 7110/7115, multiple servers can be supported. In this configuration, the 7110/7115 sits between the router and the switch. SSL traffic intended for these servers is intercepted and other traffic is passed through.

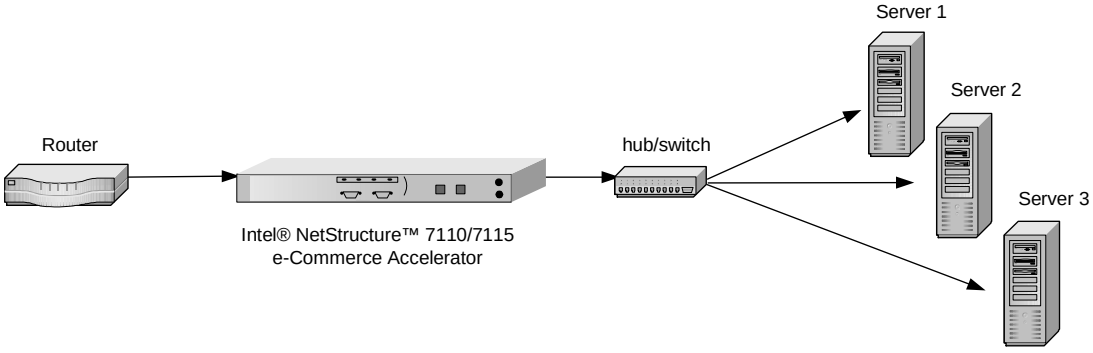

Figure 3-2: 7110/7115 in Multiple Server Configuration

Working with Internet Traffic Management (ITM) Devices

The 7110/7115 is compatible with Internet Traffic Management (ITM) devices. In such environments, the 7110/7115 lies between the router and the ITM device, or between the ITM device and the server. ITM devices distribute workload across multiple servers and redirect traffic based on content.

Positioning 7110/7115 between ITM Device and Client Network

If the ITM device supports layer 7 traffic management, URLs must be readable (that is, unencrypted), thus in environments performing layer 7 load balancing, it is recommended that the 7110/7115 be placed between the ITM device and the client network.

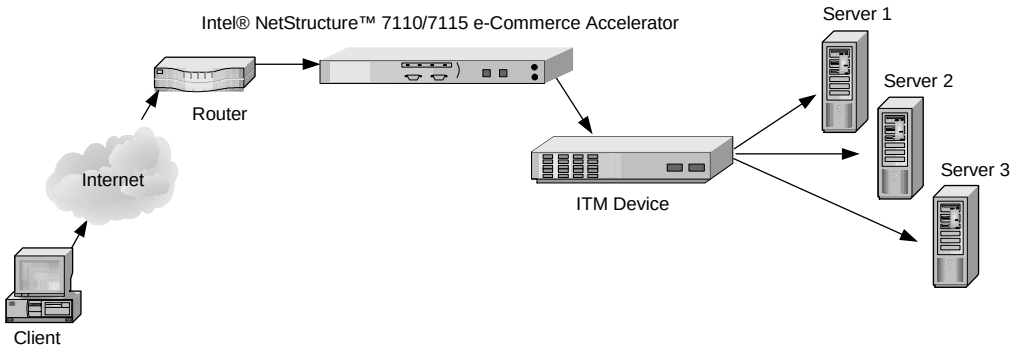

Figure 1-3: 7110/7115 Between Router and ITM Device

Positioning 7110/7115 between ITM Device and Server

If security considerations require limited network access to clear text, the 7110/7115 should be placed between the ITM device and the server.

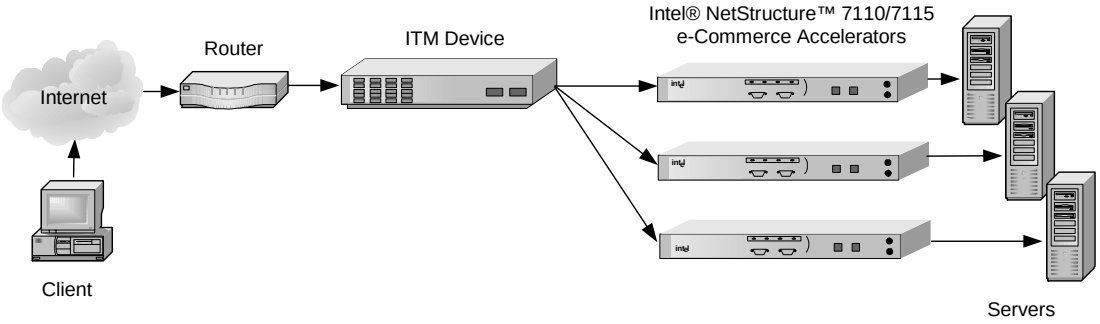

Figure 1-4: 7110/7115s Between ITM Device and Servers

NOTE: *The configuration in Figure 1-4 precludes layer 7 load balancing because secure traffic through the ITM device is encrypted.*

Multiple 7110/7115s and Cascading Processing

Scalability and Cascading

The 7110/7115's capabilities are scalable by chaining, or "cascading," multiple 7110/7115s together. In such configurations, each unit's server side connector is wired to the network side connector of the next 7110/7115 in line. The last 7110/7115 in line is connected to the server, switch, or ITM device.

Spilling and Throttling

When the 7110/7115's "spill" option is enabled, if a given 7110/7115 cannot process a request within a specified interval, the request is passed on, still encrypted, to the next 7110/7115 in line. The last

7110/7115 on the server side can also be enabled to spill to the server. Spilling is performed dynamically on a connection-by-connection basis. (See **spill** command, Chapter 5, "Command Reference.") If spill is disabled, the 7110/7115 "throttles," that is, will not accept incoming requests when it becomes overloaded.

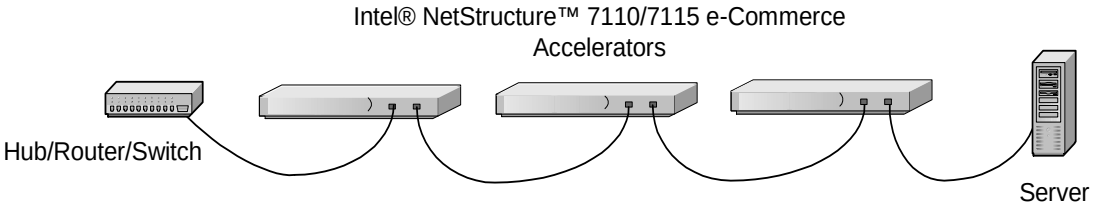

Figure 3-5: Cascaded 7110/7115s

Availability

When a 7110/7115 fails or is set to Bypass mode while Fail-through is enabled, the 7110/7115's network side and server side network adapters are directly connected, allowing traffic to pass through to the next device until the failed unit is brought back into service. This feature eliminates a single point of failure and provides a high level of availability, should there be a failure. In installations with multiple 7110/7115s, the next unit in the cascade picks up the encryption/ decryption workload, while in single 7110/7115 configurations, the server assumes the load. See"*Failure/Bypass Modes* in Appendix B for more information.

Keys and Certificates

WARNING: *The 7110/ 7115 comes with default keys and certificates for test purposes, however certificates for production use should be obtained from a recognized certificate authority.*

A necessary part of the 7110/7115 configuration is the use of keys and certificates. A key is a set of numbers used to encrypt or decrypt data. A certificate is a "form" that identifies a server or user. The certificate contains information about your company as well as information from a third party that verifies your identity.

There are three ways to obtain keys and certificates:

- Obtaining a certificate from VeriSign§ or other certificate authority
- Using an existing key/certificate
- Creating a new key/certificate on the 7110/7115

Cutting and Pasting with HyperTerminal§

Cutting and pasting is an integral part of the next several procedures. Below are procedures for cutting and pasting in HyperTerminal§. If you use some other terminal program, consult that product's documentation for appropriate procedures.

To copy an item (key, certificate signing request, etc.) from HyperTerminal§:

1. Open the HyperTerminal§ window.
2. Click and drag to select the item.
3. After the item is selected, open the **Edit** menu and click **Copy** (or type <**ctrl-c**>).
4. Open the window where you will paste the data, and position the cursor at the appropriate point.
5. In the **Edit** menu, click **Paste** (or type <**ctrl-v**>).

To paste an item (key, certificate signing request, etc.) into HyperTerminal§:

1. Display the item in the appropriate application window, then click and drag to select the item.
2. Once the item is selected, click the **Edit** menu and select **Copy** (or type <**ctrl-c**>).
3. Move to the HyperTerminal§ window, and position the cursor at the appropriate point.
4. Pull down the **Edit** menu, and select **Paste to Host** (or type <**ctrl-v**>).

Obtaining a Certificate from VeriSign§ or Other Certificate Authority

Use the **create key** command to create your key and the **create sign** command to create a signing request to be sent to VeriSign or other certificate authority for authentication. The certificate authority will return it in approximately one to five days. After you have received the certificate, use the **import cert** command to import it into the 7110/7115.

The fields input to create a signing request are called collectively a Distinguished Name (DN). For optimal security, one or more fields must be modified to make the DN unique.

Procedure

Create a key:

1. Type the **create key** command at the prompt:

```
Intel 7115> create key
Key strength (512/1024) [512]:
New keyID [001]: 002
Keypair was created for keyID: 002
```

2. Create a Certificate Signing Request:

```
Intel 7115> create sign 002
You are about to be asked to enter information
that will be incorporated into your
certificate request. The "common name" must be
unique. For other fields, you could use
default values.
```

Certifying authorities have specific guidelines on how to answer each of the questions. These guidelines may vary by certifying authority. Please refer to the guidelines of the certifying authority to whom you submit your Certificate Signing Request (CSR). Please keep the following in mind when entering the information that will be incorporated into your certificate request:

- **Country code**: This is the two-letter ISO abbreviation for your country (for example, US for the United States).
- **State or Province**: This is the name of the state or province where your organization's head office is located. Please enter the full name of the state or province. Do not abbreviate.

- **Locality**: This is usually the name of the city where your organization's head office is located.
- **Organization**: This should be the organization that owns the domain name. The organization name (corporation, limited partnership, university, or government agency) must be registered with some authority at the national, state, or city level. Use the legal name under which your organization is registered. Please do not abbreviate your organization's name and do not use any of the following characters: < > ~ ! @ # $ % ^ * / \ ( ) ?.
- **Organizational unit**: This is normally the name of the department or group that will use the certificate.
- **Common name**: The common name is the "fully qualified domain name," (or FQDN) used for DNS lookups of your server (for example, www.mysite.com). Browsers use this information to identify your Web site. Some browsers will refuse to establish a secure connection with your site if the server name does not match the common name in the certificate. Please do not include the protocol specifier "http://" or any port numbers or pathnames in the common name. Do not use wildcard characters such as * or ?, and do not use an IP address.
- **E-mail address**: This should be the e-mail address of the administrator responsible for the certificate.

3. Export the Certificate Signing Request (CSR).

In this example, xmodem is used to send the CSR to a PC connected to the console port.

```
Intel 7115> export sign mywebserver
Export protocol: (xmodem, uuencode, ascii)
[ascii]:x <Enter>
Use Ctrl-x to kill transmission
Beginning export...
Export successful!
Intel 7115>
```

To submit the CSR to a certifying authority, paste it into the field provided in the authority's online request form. Remember to include the "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE REQUEST-----" lines.

Typically, the CSR will look something like this:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBnDCCAQUACQAwXjELMAkGA1UEBhMCQ0ExEDOABgNVBAgT
B09udGFayW8xEDAOBgNVBAcTB01vbnRyYWwxDDAKBgNVBAoT
A0tGQzEdMBsGA1UEAxMUd3d3Lmlsb3ZlY2hpY2tlbi5jb20w
gZ0wDQYJKoZIhvcNAQEBBQADgYsAMIGHAoGBALmJA2FLSGJ9
iCF8uwfPW2AKkyyKoe9aHnnwLLw8WWjhl[ww9pLietwX3bp6
Do87mwV3jrgQ1OIwarj9iKMLT6cSdeZ0OTNn7vvJaNv1iCBW
GNypQv3kVMMzzjEtOl2uGl8VOyeE7jImYj4HlMa+R168AmXT
82ubDR2ivqQwl7AgEDoAAwDQYJKoZIhvcNAQEEBQADgYEAn8
BTcPg4OwohGIMU2m39FVvh0M86ZBkANQCEHxMzzrnydXnvRM
KPSE208x3Bgh5cGBC47YghGZzdvxYJAT1vbkfCSBVR9GBxef
6ytkuJ9YnK84Q8x+pS2bEBDnw0D2MwdOSF1sBb1bcFfkmbpj
N2N+hqrrvA0mcNpAgk8nU=
-----END CERTIFICATE REQUEST-----
```

4. When the certificate authority returns the certificate, import it into the 7110/7115. Use the **import cert** command, with the KeyID. As with the import key, choose an import protocol for importing the key. Use **p** for paste. After the paste is finished, add three periods to display the command line.

```
Intel 7115> import cert mywebserver
keyid is mywebserver;
Import protocol: (paste, xmodem, uudecode)
[paste]: <Enter>
Type or paste in date, end with ... alone on line

-----BEGIN CERTIFICATE-----
MIIDKDCCAtKgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBnDEL
MAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMQ4wDAYDVQQHEwVQ
b3dheTEaMBgGA1UEChMRQ29tbWVyY2Ug
.
.
.
-----END CERTIFICATE----- <Enter>

... <Enter>
Import successful!
Intel 7115>
```

5. Create mapping for Server 1. Use the **create map** command to specify the server IP address, ports, and keyID.

```
Intel 7115> create map
Server IP (0.0.0.0): 10.1.1.30
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: mywebserver
```

6. Save the configuration when the server has been mapped.

```
Intel 7115> config save
Saving configuration to flash...
Configuration saved to flash
Intel 7115>
```

Using an Existing Key/Certificate

Exporting a Key/Certificate from a Server

This method is used when it is important that the existing keys and certificates are used.

NOTE: *Currently there is no published method for extracting private keys from Microsoft IIS or Netscape servers.*

Consult your server software documentation for detailed instructions on how to export keys and certificates. Once you have exported the keys and certificates, use the **import key** and **import cert** commands to paste the keys and certificates into your 7110/7115. Some general instructions are provided below for the Apache Web Server.

Apache Interface to Open SSL§ (mod_ssl)

For key:

1. Look in $APACHEROOT/conf/httpd.conf for location of *.key file.
2. Copy and paste the key file.

For certificate:

1. Look in $APACHEROOT/conf/httpd.conf for location of *.crt file (certificate).
2. Copy and paste the certificate file.

Apache SSL§

For key:

1. Look in $APACHESSLROOT/conf/httpd.conf for location of *.key file.
2. Copy and paste the key file.

For certificate:

1. Look in $APACHESSLROOT/conf/httpd.conf for location of *.cert file.
2. Copy and paste the certificate file.

Stronghold§

For key:

1. Look in $STRONGHOLDROOT/conf/httpd.conf for location of *.key file.
2. Copy and paste the key file.

For certificate:

1. Look in $STRONGHOLDROOT/conf/httpd.conf for location of *.cert file.
2. Copy and paste the certificate file.

Importing into the 7110/7115

1. Use the **import key** command with the keyID, and choose an import protocol for importing the key. In this case, use the default to "paste." When the paste is finished, add a line break followed by three periods to display the command line.

```
Intel 7115> import key mywebserver
Import protocol: (paste, xmodem, uudecode)
[paste]: <Enter>
Type or paste in date, end with ... alone on line

-----BEGIN RSA PRIVATE KEY-----
MIIBOgIBAAJBALGOlBH14vIdtfuA+UnyRIoKya13ey8mj3GD
QakdwoDJALu+jtcC
.
.
.
S9dPdwp6zctsZeztn/ewPeNamz3q8QoEhY8CawEA

-----END RSA PRIVATE KEY-----<Enter>

... <Enter>
Import successful!
Intel 7115>
```

2. Use the **import cert** command with the keyID. As with import key, choose an import protocol for importing the key. Use the default to "paste." When the paste is finished, add a line break followed by three periods to display the command line.

```
Intel 7115> import cert mywebserver
keyid is mywebserver;
Import protocol: (paste, xmodem, uudecode)
[paste]: <Enter>
Type or paste in date, end with ... alone on line

-----BEGIN CERTIFICATE-----
MIIDKDCCAtKgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBnDEL
MAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMQ4wDAYDVQQHEwVQ
b3dheTEaMBgGA1UEChMRQ29tbWVyY2Ug
.
.
.
-----END CERTIFICATE----- <Enter>

... <Enter>
Import successful!
Intel 7115>
```

3. Create a server mapping. Use the **create map** command to specify the server IP address, ports, and keyID.

```
Intel 7115> create map
Server IP (0.0.0.0): 10.1.1.30
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: mywebserver
```

4. Save the configuration when the server has been mapped.

```
Intel 7115> config save
Saving configuration to flash...
Configuration saved to flash
Intel 7115>
```

Creating a new Key/Certificate on the 7110/7115

Use the **create key** and **create cert** commands to create new keys and certificates for 7110/7115 operation. This procedure can be used when there are no existing keys and certificates on the server. The advantage is that this method is very fast, but a certificate authority has not signed the certificates.

The fields input to create a certificate are called a Distinguished Name (DN). For optimal security, one or more fields must be modified to make the DN unique.

Procedure

1. Create a key as follows:

```
Intel 7115> create key
Enter the key strength [512,1024]: 512
New keyID [001]: mywebserver
Keypair was created for keyID: mywebserver
```

2. Enter the **create cert** command with the keyID

```
Intel 7115> create cert mywebserver
You are about to be asked to enter information...
```

Enter the information for the certificate, as prompted:

- Country
- State
- Locality
- Organization
- Organization unit
- Common name (for example, www.myserver.com)
- E-mail address.

3. Create a server mapping. Use the **create map** command to specify the server IP address, ports, and keyID.

```
Intel 7115> create map
Server IP (0.0.0.0): 10.1.1.30
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: mywebserver
```

4. Save the configuration when the server has been mapped.

```
Intel 7115> config save
Saving configuration to flash...
Configuration saved to flash
Intel 7115>
```

Global Site Certificates

Overview

Four types of certificates are involved in the following discussion:

- Root Certificate. The certificate of a trusted CA such as VeriSign.
- Server Certificate. Loaded on the server. Can be either self-generated or received from a certificate authority such as VeriSign. Interacts with requesting browser's root certificate to establish encryption level.
- Global Site Certificate. An extended server certificate. Allows 128-bit encryption for export-restricted browsers.
- Intermediate certificate authority (CA) Certificate. A certificate "signed," that is, authenticated, by a recognized certificate authority such as VeriSign, and used to validate a global site certificate. Called an "intermediate CA certificate" in the following discussion.

Export versions of Internet Explorer§ and Netscape§ Communicator use 40-bit encryption to initiate connections to SSL servers. Upon receiving a client request, the server responds by sending a digital certificate. If this certificate is a conventional server certificate (that is, not a global site certificate), browser and server complete the SSL handshake and use a 40-bit key to encrypt application data. If the server responds to a requesting browser with a global site certificate, the client automatically renegotiates the connection to use 128-bit encryption.

A global site certificate is validated by an accompanying intermediate CA certificate. (Such pairs are called “chained certificates.”) Examples of intermediate CA certificates include Microsoft SGC Root§, and VeriSign Class 3§ CA. When a requesting browser receives a global site certificate along with an intermediate CA certificate, the browser’s root certificate is used to validate the intermediate CA certificate, which in turn is used to validate the global site certificate, thus letting the browser know that it can renegotiate the connection to use 128-bit encryption.

Global Site Certificate Paste Procedure

If you wish to use a global site certificate, you must import both the global site certificate and its accompanying intermediate CA certificate. Both certificates must be chained together in a single file.

Use the **import cert** command to import either single or chained certificates. In the latter case, paste the server’s global site certificate first, followed by the intermediate CA certificate. Follow the intermediate CA certificate by typing three periods on a new line.

Example:

```
Intel 7115> import cert <keyID>
Import protocol: (paste, xmodem, uudecode)
[paste]:
Type or paste in data, end with ... alone on line

-----BEGIN CERTIFICATE-----
MIIFZTCCBM6gAwIBAgIQCTN2wvQH2CK+rgZKcTrNBzANBgkq
hkiG9w0BAQQFADCBujEfMB0GA1UEChMWVmVyaVNpZ24gVHJ1
c3QgTmV0d29yazEXMBUGA1UECxMOVmVyaVNpZ24sIEluYy4x
MzAxBgNVBAsTKlZlcmlTaWduIEludGVybmF0aW9uYWwgU2Vy
:
dmVyIENBIC0gQ2xhc3MgMzFJMEcGA1UECxNAd3d3LnZlcmlz
aWduLmNvbS9DUFMg
SW5jb3JwLmJ5IFJlZi4gTElBQklMSVRZIExURC4oYyk5NyBW
ZXJpU2lnbjAeFw05
OTExMTEwMDAwMDBaFw0wMDExMTAyMzU5NTlaMIHHMQswCQYD
VQQGEwJVUzETMBEG
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEMTCCA5qgAwIBAgIQI2yXHivGDQv5dGDe8QjDwzANBgkq
hkiG9w0BAQIFADBfMQswCQYDVQQGEwJVUzEXMBUGA1UEChMO
VmVyaVNpZ24sIEluYy4xNzA1BgNVBAsTLkNsYXNzIDMgUHVi
bGljIFByaW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkw
HhcNOTcwNDE3MDAwMDAwWhcN
```

NOTE: There must be no white space before, between, or after certificates, and the “Begin...” headers and “End...” trailers must all be retained.

```
:
OTk3IFZlcmlTaWduMA0GCSqGSIb3DQEBAgUAA4GBALiMmMMr
SPVyzWgNGrN0Y7uxWLaYRSLsEY3HTjOLYlohJGyawEK0Rak6
+2fwkb4YH9VIGZNrjcs3S4bmfZv9jHiZ/4PC/
NlVBp4xZkZ9G3hg9FXUbFXIaWJwfE22iQYFm8hDjswMKNXRj
M1GUOMxlmaSESQeSltLZl5lVR5fN5qu
-----END CERTIFICATE-----<Enter>
...<Enter>
Import successful!
Intel 7115>
```

Redirection: Clients and Unsupported Ciphers

NOTE: *The user must provide the redirect URL and ensure that it is available, as well as define the content of the redirect page.*

WARNING: *If the redirect URL causes a client to access the same 7110/7115 mapping that invoked the redirection an infinite loop condition will occur.*

When a client that does not support the selected cipher suite attempts to connect to the 7110/7115, the default behavior is to reject the connection, resulting in the client system reporting a fatal error. However, the 7110/7115 allows you to specify a "redirect address" where you can provide clients with additional information. The **set redirect** command allows you to specify a redirect Web address for any Map ID. The **show redirect** command displays any redirect addresses currently configured.

```
Intel 7115> list map
Map               Net  Ser  Cipher  Re-   Client
ID KeyID Server IP Port Port Suites  direct Auth
== ===== ========= ==== ==== ======  =====  ====
1  default Any     443  80   all(v2+v3) n   n
2  sample 10.1.2.5 443  80   med(v2+v3) n   n
Intel 7115> set redirect 2
Enter a redirect URL at following prompt
e.g. http://www.e-comm_site.com/weakbrowser.html
Enter redirect URL []:http://www.e-
comm_site.com/cipher_info.html
```

```
Intel 7115> list map
Map               Net  Ser  Cipher  Re-   Client
ID KeyID Server IP Port Port Suites  direct Auth
== ===== ========= ==== ==== ======  =====  ====
1  default Any     443  80   all(v2+v3) n    n
2  sample 10.1.2.5 443  80   med(v2+v3) y    n
Intel 7115> show redirect 2
Redirect URL for map 2 is set: http://www.e-
comm_site.com/cipher_info.html
```

To disable a redirect URL for a mapping:

```
Intel 7115> set redirect 2 none
Intel 7115> show redirect 2
Redirect URL for map 2 is not set
```

Client Authentication

NOTE: The 7110/7115 supports only one root CA certificate per mapping. However, multiple intermediate CA certificates per single mapping are supported.

By default, the 7110/7115 does not authenticate client identities, however specific map IDs can be configured to request client certificates for the purpose of verifying identities. When this feature is enabled, the 7110/7115 verifies that client certificates are signed by a known CA. This feature is controlled by the **import client_ca** command.

Example:

First, use the **list map** command to display the current map IDs and their configurations including, in the last column, Client Authentication, enabled (y) or disabled (n).

```
Intel 7115> list map
Map               Net  Ser  Cipher  Re-   Client
ID KeyID Server IP Port Port Suites  direct Auth
== ===== ========= ==== ==== ======  =====  ====
1 default Any       443  80  all(v2+v3) n      n
2 sample  10.1.2.57 443  80  med(v2+v3) n      n
```

Next, import the client CA certificate for Map ID 2.

```
Intel 7115> import client_ca 2

Import protocol: (paste, xmodem, uudecode)
[paste]: <Enter>

Type or paste in data, end with ... alone on line

-----BEGIN CERTIFICATE-----

MIIDxzCCAzCgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBpDEL
MAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExEjAQ
BgNVBAcTCVNhbiBEaWVnbzEUMBIGA1UE

.

.

.

XcCabZcfBRuYcZeUoNrGUl8tD80jp2YNG1vidgLEaD1YCli5
I9/mNrcB25mSfdAR

/08ROTMxm4VKOSA=

-----END CERTIFICATE-----<Enter>

...<Enter>
```

Verify the import by using the **list map** command again. Note that the Client Auth column now shows client authentication for Map ID 2 enabled.

```
Intel 7115> list map

Map                Net  Ser  Cipher  Re-   Client
ID KeyID Server IP Port Port Suites  direct Auth
== ===== ========= ==== ==== ======  =====  ====
1 default Any        443  80  all(v2+v3) n      n
2 sample  10.1.2.57 443  80  med(v2+v3) n      y
```

Clients connecting to “map 2” are required to present a client certificate signed by the CA whose certificate was imported above. If they do not present a properly signed certificate, their connection attempt is refused.

Creating a Client CA Certificate using OpenSSL§

NOTE: *To acquire a copy of OpenSSL§ for your environment, access the OpenSSL§ Web site at www.openssl.org*

There are software packages available that handle the details of client certificate generation, however, you can implement them manually. The following example illustrates the appropriate steps using OpenSSL§:

1. Generate the key pair for the client CA:

   ```
   openssl genrsa -out ca_key.pem 1024
   ```

2. Generate the client CA certificate:

   ```
   openssl req -new -x509 -config intel.cnf -key
   ca_key.pem -days 365 -out ca_cert.pem
   ```

NOTE: *In this example, ca_cert.pem is your trusted CA and signing certificate*

3. Using the **import client_ca** command, import ca_cert.pem

For each client:

1. Generate a key pair:

   ```
   openssl genrsa -out key.pem 1024
   ```

2. Generate a certificate signing request:

   ```
   openssl req -new -config intel.cnf -days 365
   -key key.pem -out csr.pem
   ```

3. Sign the client certificate signing request with the client CA certificate:

   ```
   openssl x509 -req -CAcreateserial -CAkey
   ca_key.pem -CA ca_cert.pem -days 365 -in csr.pem
   -out cert.pem
   ```

4. Convert from PEM to PKCS12 format in signed certificate form:

   ```
   openssl pkcs12 -export -in cert.pem -inkey
   key.pem -name "<Client ID>" -out cert.p12
   ```

5. Import the output file from step 4, cert.p12, the signed certificate, into the client browser.

SSL Processing

The Intel® NetStructure™ 7110/7115 e-Commerce Accelerator handles several SSL protocols, for example, HTTPS (which is the default). For security purposes, you can block access to specified IPs or ports (see “Blocking” section). Traffic that is not mapped or blocked flows through transparently (see “Failure” section). Supported protocols are listed below. (Ports listed are “well-known” port assignments. Any available port may be used.)

- HTTPS 443 (default)
- IMAPS 993
- POP3S 995
- SMTPS 465
- NNTPS 563
- LDAPS 636

Mapping

NOTE: *The 7110 supports a maximum of 100 mappings, while the 7115 supports up to 1000.*

Keypairs and their associated certificates are referenced by a keyID. A server is identified by a unique combination of server IP and network port. *Mapping* is the process of associating a keyID with a server (using server IP, network port, and server port). The 7110/7115 supports two types of mapping:

- Automapping
- Manual mapping

Automapping

NOTE: *Remember to save the configuration (with the* ***config save*** *command) after making mapping changes.*

Automapped entries are identified by a server IP address of zero (0.0.0.0). When a server IP address of zero is specified, the 7110/7115 intercepts packets to any server IP address with the matching network ports. As with any mapping entry, the combination of server IP address and network port must be unique.

The initial configuration for the 7110/7115 provides an automapping entry for network port 443 and server port 80. This is associated with the internally generated default keypair and certificate with the keyID

of “default.” Under this initial configuration, automapping occurs on any server with this network port (443) when traffic is routed through the 7110/7115.

Automapping with user-specified key and certificate

When a user-specified key and certificate are to be automapped, the user can replace the initial automapping entry with the **create map** command. By specifying the same unique identifier (server IP of 0.0.0.0, and network port of 443 with a user-generated keyID, the user can overwrite the initial automapping entry. (The key and certificate may be obtained through any of the methods described previously in this chapter.)

Automapping with multiple port combinations

The user can specify multiple automapping entries when the network port is unique. For example, a user might specify, in addition to the initial network (443) and server (80) port combination, a combination of network (8010) and server (80) port.

Deleting automapping entries

Any automapping entry can be deleted, but if the initial automapping is deleted and no other mapping entry is specified, the 7110/7115 automatically recreates the initial automapping entry. Either replace the initial automapping entry or create another mapping/automapping entry and then delete the initial automapping entry using the **delete map** command.

Manual mapping

The user can create (with the **create map** command) one or more mapping entries for individual servers. This is the only way to specify unique keyIDs for each server. Normally, when manual mapping is performed, the initial automapping entry is deleted, but this is not a requirement.

Combining automapping and manual mapping

NOTE: If both manual mappings and applicable automappings are available, the 7110/7115 ***always*** *uses the manual mapping.*

Any combination of automapping and manual mapping entries, up to a total of 1000, can be used provided the server IP address and network port combinations are unique. Several of the scenarios in Chapter 4 include step-by-step mapping procedures.

Blocking

NOTE: Blocking is always performed before mapping.

For security purposes, the 7110/7115 allows the blocking of particular IP addresses and ports. IP/port combinations can be blocked on the basis of:

- Specific IP, specific port
- Subnet of IPs, specific port
- All IPs, specific port

Specific IP, Specific Port

To block a specific server IP and specific port combination:

1. Type the **create block** command.
2. Type the IP address.
3. Press **Enter** to accept the default IP mask
4. Type the specific port.
5. Press **Enter** to accept the default port mask.

Example:

```
Intel 7115> create block
Client IP to block [0.0.0.0]: 10.1.2.1
Client IP mask [0.0.0.0]: 255.255.255.255
Server IP to block [0.0.0.0]: 20.1.2.1
Server IP mask [0.0.0.0]: 255.255.255.255
Server Port to block: 80
Server Port mask [0xffff]:<Enter>
```

Use the **show block** command to verify:

```
Intel 7115> show block
(1) block 10.1.2.1 255.255.255.255 20.1.2.1
255.255.255.255 80 0xffff
```

Subnet IP, Specific Port

To block a subnet IP, and specific port combination:

1. Type a subnet IP address, using **0** as the final octet. (In the example below, all IPs from "10.1.x.x" to "20.1.x.x" are blocked on port 80.)
2. Type the subnet mask, with **0** indicating the portion of the IP address to be ignored.
3. Type the specific port.
4. Press **Enter** to accept the default port mask.

Example:

```
Intel 7115> create block
Client IP to block [0.0.0.0]: 10.1.2.1
Client IP mask [0.0.0.0]: 255.255.0.0
Server IP to block [0.0.0.0]: 20.1.2.1
Server IP mask [0.0.0.0]: 255.255.0.0
Server Port to block: 80
Server Port mask [0xffff]:<Enter>
```

Use **show block** to verify:

```
Intel 7115> show block
-----------

blocks :

-----------

(1) block 10.1.2.1 255.255.0.0 20.1.2.1
255.255.0.0 80 0xffff

-----------
```

All IPs, Specific Port

To block a specific port on all IP addresses:

1. Type all zeroes as the IP address to be blocked.
2. Type all zeroes as the IP wildcard mask to be blocked.
3. Type the specific port.
4. Press **Enter** to accept the default port mask.

Example:

```
Intel 7115> create block
Client IP to block [0.0.0.0]: <enter>
Client IP mask [0.0.0.0]: <enter>
Server IP to block [0.0.0.0]:<enter>
Server IP mask [0.0.0.0]:<Enter>
Server Port to block: 80
Server Port mask [0xffff]:<Enter>
```

5. Use the **show block** command to confirm the block:

```
Intel 7115> show block
-----------

blocks :

-----------

(1) block

0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 80 0xffff

-----------
```

Delete a Block

The example below illustrates how to delete a subnet block. Type the **delete block** command with the block ID (block ID is **1** in the example):

1. Use the **show block** command to identify the block to be deleted.

```
Intel 7115> show block
-----------

blocks :

-----------

(1) block 10.1.2.1 255.255.255.255 20.1.2.1
255.255.255.255 80 0xffff

-----------
```

2. Use the **delete block** command followed by the block ID to delete the block.

```
Intel 7115> delete block 1
```

Failure Conditions, Fail-safe, and Fail-through

During any failure condition of the 7110/7115, unprocessed data packets can either pass through or not, depending on whether Fail-safe or Fail-through mode is enabled. The Fail-through switch is by default in Fail-safe mode, meaning that during a failure no data packets will pass from one side of the 7110/7115 to the other. For details, see “Failure/Bypass Modes” in Appendix B.

4 Scenarios

This section contains scenarios illustrating examples of Intel® NetStructure™ 7110/7115 e-Commerce Accelerator configurations:

- Scenario 1: Single server
- Scenario 2: Multiple servers
- Scenario 3: Multiple 7110/7115s, cascaded
- Scenario 4: Different ingress and egress routers

Syntax

The CLI uses the following syntax:

Symbol	Significance
Angled brackets (< >)	Angled brackets designate where you type variable parameters.
Straight brackets ([ ])	Choices of parameters appear between straight brackets, separated by vertical bars.
Braces ({})	Optional commands or parameters appear between braces.
Boldface	Commands shown as they are typed after the CLI prompt appear in **boldface** type. (The prompt appears in normal typeface to distinguish it from the command text.)
Vertical bar (|)	Separates choices of input parameters within straight brackets. You can choose only one of a set of choices separated by the vertical bar. (Do not include the vertical bar in the command.)

Scenario 1—Single Server

This scenario describes a typical configuration of a 7110/7115 with one server, using either automapping or manual configuration/ mapping. This scenario describes the fastest way to get up and running with a 7110/7115.

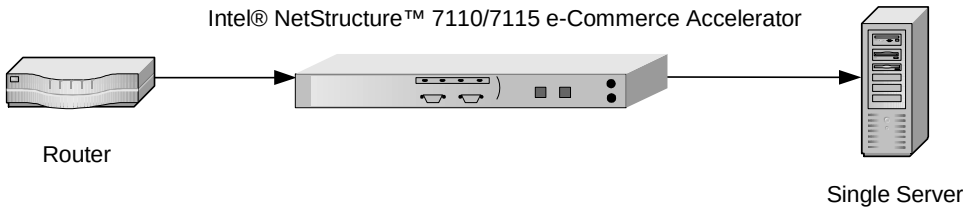

Figure 4-1: Single 7110/7115, Single Server Installation

Procedure for Scenario 1

Automapping

1. Physically connect the 7110/7115 to the router and to one server.
2. Initiate HTTPS traffic to the server. The 7110/7115 monitors traffic and uses the initial mapping (with associated default key and certificate) to decrypt HTTPS traffic and pass clear text HTTP traffic to the server.

Manual Configuration

1. Perform the installation as described in Chapter 2. Access the 7110/7115 command prompt.
2. Acquire the appropriate keys and certificates following the procedure in the “Keys and Certificates” section in Chapter 3.

3. Create a mapping for the server. Use the **create map** command to specify the server IP address, ports, and keyID.

```
Intel 7115>create map
Server IP (0.0.0.0): 10.1.1.30
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: myserver
```

4. You can delete the default mapping. After the user has manually created the mapping, the default mapping can be deleted. In this case, delete MapID number 1. MapID number 2 becomes MapID number 1 when the default is deleted.

```
Intel 7115>delete map 1
Intel 7115>list maps

Map                Net Ser Cipher Re-   Client
ID KeyID  Server IP Port Port Suites direct Auth

== =====  ========= ==== ==== ======  =====  ====

1  myserver 10.1.1.30 443 80 med(v2+v3) n   n
Intel 7115>
```

5. Save the configuration when the server has been mapped.

```
Intel 7115>config save
Saving configuration to flash...
Configuration saved to flash
Intel 7115>
```

Scenario 2—Multiple Servers

This scenario shows how to configure two or more servers.

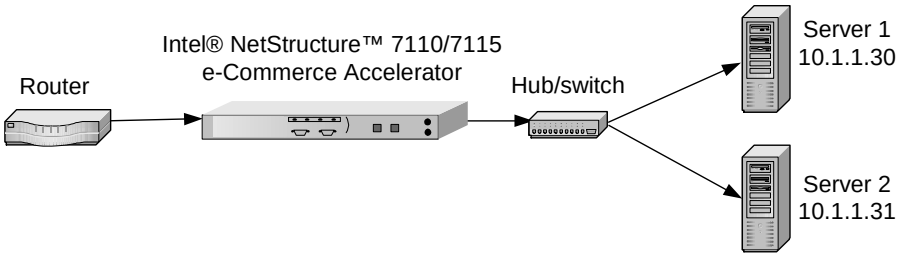

Figure 4-2: Single 7110/7115, Multiple Server Installation

Procedure for Scenario 2

1. Perform the installation as described in Chapter 2. Access the 7115 command prompt.
2. Acquire the appropriate keys and certificates following the procedure in the *Keys and Certificates* section in Chapter 3.
3. Create a mapping for Server 1. Use the **create map** command to specify the server IP address, ports, and keyID.

```
Intel 7115>create map
Server IP: 10.1.1.30
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: myserver
```

4. Create a mapping for Server 2. As in the previous step, use the **create map** command to specify the server IP address, ports for the second server, and the keyID.

```
Intel 7115>create map
Server IP: 10.1.1.31
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: myserver
```

5. Use the **list map** command to view the mapping. (Multiple keys and certificates can also be imported and each mapped to individual servers. If you do this, at least one field in the certificate information—usually the common name—must be unique.)

```
Intel 7115> list map

Map                Net Ser Cipher Re-   Client
ID KeyID  Server IP Port Port Suites direct Auth

== =====  ========= ==== ==== ======  =====  ====

1 default  Any       443 80   all(v2+v3) n   n
2 myserver 10.1.1.30 443 80   med(v2+v3) n   n
3 myserver 10.1.1.31 443 80   med(v2+v3) n   n
Intel 7115>
```

6. After you have manually created a mapping, the default mapping can be deleted. In this case, delete MapID number 1. MapID number 2 becomes MapID number 1 when the default is deleted.

```
Intel 7115>delete map 1
Intel 7115>list map

Map                Net Ser Cipher Re-   Client
ID KeyID  Server IP Port Port Suites direct Auth

== =====  ========= ==== ==== ======  =====  ====

1 myserver 10.1.1.30 443 80   med(v2+v3) n   n
2 myserver 10.1.1.31 443 80   med(v2+v3) n   n
Intel 7115>
```

7. To configure a third or fourth web server to operate with the 7110/7115, repeat the steps above, specifying a different IP address for each server.

8. Save the configuration when mapping is completed for the server(s).

```
Intel 7115>config save
Saving configuration to flash...
Configuration saved to flash
Intel 7115>
```

Scenario 3—Multiple 7110/7115s, Cascaded

This scenario shows how to cascade 7110/7115s for additional performance and availability. The same procedures apply that were performed in Scenario 3. In addition, the complete configuration of the first 7110/7115 is exported to the second 7110/7115 in line.

Assumptions

- Two or more 7110/7115s must be physically installed on the same network. To cascade multiple 7110/7115s, connect from the server port of the first 7110/7115 to the network port of the next 7110/7115 in line, and then again connect from the server port to the network port of the next 7110/7115 in line, or to the server. (See Chapter 2: Installation for more information.)
- On the first 7110/7115, the **set spill enable** command is used to enable spilling so that the next 7110/7115 in line can handle the overflow. Spill is then enabled for each subsequent 7110/7115, except the last one. Do not configure the last 7110/7115 to spill to the server.
- The first 7110/7115 should be fully configured; any necessary keys, certificates or maps must exist. The complete configuration is exported from the first, then imported to the next 7110/7115 in line. This procedure is repeated for any additional 7110/7115s in line.

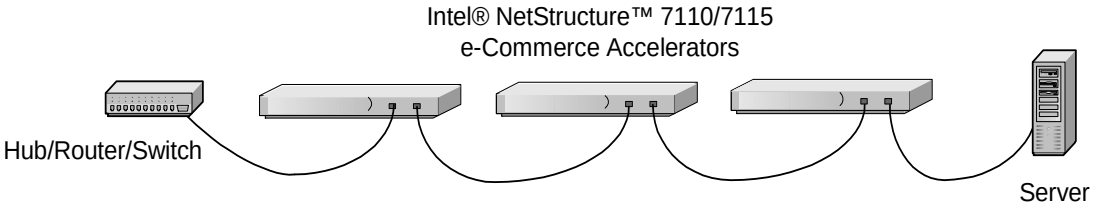

Figure 4-3: Multiple (Cascaded) 7110/7115s

Procedure for Scenario 3

1. Configure the 7110/7115 farthest from the server as described in any of the preceding scenarios. Remain connected to that specific 7110/7115 for the export configuration procedure.
2. At the command prompt, type the **set spill enable** command. This allows overflow traffic to be transferred to the second 7110/7115 for processing.
3. Save configuration.

```
Intel 7115>config save
Saving configuration to flash...
Configuration saved to flash

Intel 7115>
```

4. Export the configuration. Use the **export config** command. Choose xmodem mode (**x**) to export.

```
Intel 7115> export config
Export protocol: (xmodem, uuencode, ascii)
[ascii]: x <Enter>
Beginning export...
```

5. Select **Receive** from the HyperTerminal§ **Transfer** menu.
6. Type or use the **Browse** button to specify the directory where you wish to place the received file.
7. Select xmodem as the receiving protocol.
8. Click the **Receive** button**.**

9. Specify a filename for the received file and click **OK**. The operation concludes and the normal prompt reappears.

```
Use Ctrl-X to kill transmission
Export successful!
Intel 7115>
```

10. Connect to the second 7110/7115, either through the console connection or another window (if both are connected to the same PC).

11. Import the configuration. Use the **import config** command to begin the process. Select xmodem (**x**) and press **Enter** to begin the import process.

```
Intel 7115> import config
Import protocol: (paste, xmodem, uudecode)
[paste]: x <Enter>
Use Ctl-X to cancel upload
```

12. Select **Send** from the HyperTerminal§ **Transfer** menu.

13. Type or use the **Browse** button to specify the file to send.

14. Select xmodem as the sending protocol.

15. Click the **Send** button. The transfer completes and then you are prompted to verify that you wish to install this configuration.

```
Do you want to install this config ? [y]: y
```

16. After verification (**y**) or refusal (**n**), the prompt reappears.

```
Intel 7115>
```

17. Save the configuration.

```
Intel 7115>config save
Saving configuration to flash...
Configuration saved to flash
Intel 7115>
```

18. Repeat steps 11-17 for any additional 7110/7115s. On the last 7110/7115 in the chain, disable spilling with the **set spill disable** command.

Scenario 4—Different Ingress and Egress Routers

This scenario describes the configuration of a 7110/7115 when the ingress and egress traffic paths are different. This scenario includes:

- One or more servers
- One or more 7110/7115s (Multiple commerce accelerators can be cascaded in this configuration.)
- One or more ingress routers
- One egress router

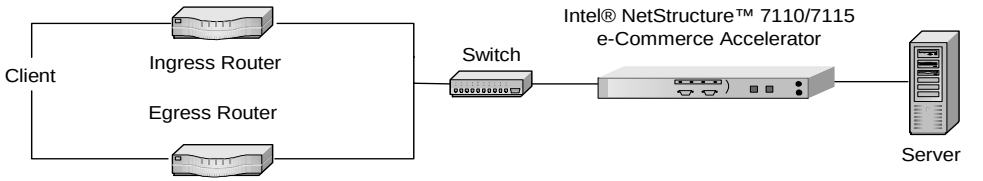

Figure 4-4: Installation with Ingress and Egress Routers

Procedure for Scenario 4

NOTE: *Execute an "arp –a" on the server to display the MAC address of the default gateway. This is the address you should use.*

1. Configure your 7110/7115 (as described in any of the previous scenarios).
2. Determine the MAC address of the egress router you wish to route outbound traffic through.
3. At the CLI prompt, enter the default egress router.

```
Intel 7115>set egress_mac 00:11:22:33:44:55
Egress MAC set to 00:11:22:33:44:55

Intel 7115>config save
Saving configuration to flash...
Configuration saved to flash
Intel 7115>
```

4. To reverse this process:

```
Intel 7115>set egress_mac none
```

5 Command Reference

The Intel® NetStructure™ 7110/7115 e-Commerce Accelerator is fully configurable through the Command Line Interface (CLI). The CLI is accessible through the console and aux console RS232 ports.

Online Help

The 7110/7115 provides online help with the following options:

- Type `help` to display a summary of commands.
- Type `help <command>` (or `? <command>`) for a description of a specific command or, if relevant, a list of subcommands you can enter from within `<command>`.
- Type `help usage` (or `? <usage>`)to display all commands and their usage.
- Type `tty_char` to display a list of special terminal editing characters.

Command Line Interface

The CLI handles all user interactions on the console and auxiliary console RS232 ports. One instance per port runs at all times.

User Authentication

To gain access to the CLI, the user must first be authenticated by providing a password at the logon banner prompt. The logon banner provides build version information and the serial number.

Command Line Prompt

The standard command line prompt for the 7115 is:

```
Intel 7115>
```

The prompt for the 7110 is:

```
Intel 7110>
```

The prompt can be changed with the **set prompt** command.

Abbreviation to Uniqueness

It is not always necessary to type the entire command. CLI commands can be abbreviated to uniqueness. For example, "**del"** as show below is sufficient to represent the **delete** command:

```
Intel 7115> del
Usage: delete item [arg]
      block     blockID
      cert      keyID
      client_ca mapID
      key       keyID
      logs      logID|all
      map       mapID
      patch
      permit    permitID
      sign      keyID
      snmp_community
      trap_community
```

However, "**sh**" as shown below, is not an abbreviation to uniqueness in that it does not distinguish between **show** and **showsnmp**.

```
Intel 7115> sh
```

The solitary letter "**e**" in the context of the next example, (i.e., preceded by "**ssh**"), uniquely indicates **ssh enable**.

```
Intel 7115> set ssh e
SSH Service started.
```

Input Editing Commands

Moving the Insertion Point

Command	Description
ctrl-b	Move back one character.
ctrl-f	Move forward one character.
ctrl-a	Move to the start of the current line.
ctrl-e	Move to the end of the line.
ctrl-l	Clear the screen and redraw the current line, leaving the current line at the top of the screen.

Command History

A history of recently executed commands is stored in a buffer and can be accessed with the following commands:

Command	Description
ctrl-r	(Reverse-search-history) Search backward starting at the current line and moving up incrementally through the command history.
ctrl-s	(Forward-search-history) Search forward starting at the current line and moving down incrementally through the command history.

Cut and Paste

Command	Description
ctrl-d	Delete the character underneath the cursor.
ctrl-k	Delete the text from the current cursor position to the end of the line.
ctrl-u	Delete backward from the cursor to the beginning of the current line.
ctrl-w	Delete the word behind the cursor, using white space as a word boundary.
ctrl-y	Copy text that has been deleted.
backspace/del	Delete the character to the left of the cursor.

Command Summary

This section contains a high-level view of the 7110/7115's command structure. Details appear in the next section, *Command Reference.*

Command	Command Options
bypass	
config	save default compare reset
create	block cert <keyID> key <keyID> map permit sign <keyID>
delete	block <blockID> cert <keyID> client_ca <mapID> key <keyID> logs<logID | all> map <mapID> patch permit <permitID> sign <keyID> snmp_community trap_community
exit	
export	cert <keyID> config key <keyID> log <logID> sign <keyID>
factory_default	
help	help help <command> help usage

Command	Command Options
import	cert <keyID> client_ca <mapID> config key <keyID> patch upgrade
inline	
list	blocks filters (shows blocks and permits) keys logs maps monitoring permits procs service snmp_community trap_community
nic	
password	
reboot	

Command	Command Options
set	alarms <all, esc, rsc, utl, ovl, nls> cache ciphers <mapID> ciphers <mapID> default client_tmo date defcert egress_mac x:x:x:x:x:x: egress_mac none ether idleto <timeout> ip <ip> <netmask> kstrength max_remote_sessions<1-5> monitoring <enable | disable> monitoring_interval monitoring_fields more ovl_window <seconds> prompt redirect <mapID> redirect <mapID> none route x.x.x.x rsc_window <seconds> serial server_tmo ssh <enable | disable> ssh_port spill <enable | disable> telnet <enable | disable> telnet_port <port> utl_high <percentage> utl_low <percentage> utl_window <seconds>

Command	Command Options
show	alarms blocks cache cert <keyID> client_ca <mapID> client_tmo config config default config saved date defcert egress_mac ether filters idleto info ip key <keyID> kstrength logs map max_remote_sessions monitoring monitoring_interval monitoring_fields more ovl_window permits rsc_window redirect <mapID> route serial server_tmo ssh ssh_port sign <keyID> spill status <arg> telnet

Command	Command Options
show	telnet_port utl_highwater utl_lowwater utl_window
setsnmp	snmp <enable | disable> snmp_community snmp_port snmp_info sys_contact sys_location sys_name trap_authen <enable | disable> trap_community trap_port
showsnmp	snmp snmp_community snmp_port snmp_info sys_contact sys_location sys_name trap_authen trap_community trap_port
status	realtime line
tty_char	

Command Reference

Help Commands

Command	Description
help	Display the list of available commands.
help <command>	Display usage for a single command.
help usage	Display all commands and their usage.
tty_char	View the available list of keyboard shortcut commands.

Status Command

Command	Description
status	Display device statistics. Several modes are available, as described below. (Default: realtime.) Syntax: `Intel 7115> status <arg>` where: <line> specifies a line-oriented display of statistics. <realtime> specifies that statistics be displayed in realtime. <alarms> shows current alarm events. <log> shows statistics and alarm events in log file.

SSL Commands

Command	Description
create key	Create a new keypair and associate it with a Key ID. **Example**: `Intel 7115> create key` `Key strength (512/1024) [512]: 1024` `New keyID [001]:<Enter>` `Keypair was created for keyID: 001.` `Intel 7115>`
delete key	Delete a specified keypair for a given Key ID. **Syntax**: `Intel 7115> delete key <keyID>` where `<keyID>` is the Key ID whose associated keypair you wish to delete.
import key	Import a keypair for the specified Key ID. **Syntax**: `Intel 7115> import key <keyID>` where `<keyID>` is the ID of the keypair you wish to import.

Command	Description
export key	Export a keypair for a specified Key ID (ASCII, xmodem, or uuencode). **Syntax**: `Intel 7115> export key <keyID>` `Export protocol: (xmodem, uuencode, ascii) [ascii]: <Enter>` `Press any key to start, then again when done...<Enter>` `-----BEGIN RSA PRIVATE KEY-----` `MIIBOgIBAAJBALqeajCDgfa8fY8FROLi0B8fVp3m4EI` `2MpOzKvEKKe6Kk5pDBkH83tUBkssGBtbnDYHkiAyGzA` `.` `.` `.` `UFFSNgBRvbkiNvaNiVqKeutwDEhgCL0PDueo` `-----END RSA PRIVATE KEY-----<Enter>` `Intel 7115>` where <keyID> is the identifier of the keypair you wish to export.
show key	Display the expanded keypair (including PEM format) for a specified Key ID. If no Key ID is specified, displays all keys. **Syntax**: `Intel 7115> show key <keyID>` where <keyID> is the Key ID whose associated keypair you wish to view.
list keys	List available Key IDs. **Example**: `Intel 7115> list keys` `001` `default` `Intel 7115>`

Command	Description
create cert	Create a new certificate for a specified Key ID. **Syntax**: `Intel 7115> create cert <keyID>` where <keyID> is the Key IDfor which you wish to create a certificate.
delete cert	Delete the certificate associated with a specified Key ID. **Syntax**: `Intel 7115> delete cert <keyID>` where <keyID> is the Key ID whose associated certificate you wish to delete.
import cert	Import a certificate to associate with a specified Key ID. **Syntax**: `Intel 7115> import cert <keyID>` where <keyID> is the Key ID whose associated certificate you wish to import.
export cert	Export the certificate for a specified Key ID. **Syntax**: `Intel 7115> export cert <keyID>` where <keyID> is the Key ID whose associated certificate you wish to export.

Command	Description
show cert	Display the expanded certificate (including PEM format) associated with a specified Key ID. If no Key ID is specified, displays all certificates. Syntax: `Intel 7115> show cert <keyID>` where `<keyID>` is the Key ID whose associated certificate you wish to view.
set ciphers	Establish the list of ciphers and cipher strengths that will be recognized by the specified Map ID. **Syntax**: `Intel 7115> set ciphers <mapID>` `1 - all` `2 - high` `3 - medium` `4 - low` `5 - export only` `6 - Customized Ciphers` `Select cipher strength [1]: 1` `1 - SSLv2` `2 - SSLv3` `3 - SSLv2 and SSLv3` `Select ciphers from SSL version [3]: 2` `Intel 7115>` where `mapID` is the identifier of the mapping whose ciphers you wish to set.

Command	Description
set redirect	Set an alternative address to which a client is directed in the event it doesn't support the specified Map ID's selected cipher suites. **Syntax**: `Intel 7115> set redirect <mapID> [none]` `Enter redirect URL []: <URL>` where <mapID> is the Map ID for which you wish to define a redirect URL, and <URL> is the Web address to which you wish to redirect clients that don't support the selected cipher suites. Enter the optional parameter [none] to disable an existing redirect URL for the specified Map ID.
show redirect	Displays the alternative address, if one is configured for the specified Map ID, to which a client is directed in the event it doesn't support the selected cipher suite. **Syntax**: `Intel 7115> show redirect <mapID>` where <mapID> is the Map ID whose redirect URL you wish to display. If no redirect address is defined, a command line message informs you of the fact: `Intel 7115> show redirect 1` `Redirect URL for map 1 is not set.` `Intel 7115>`
show client_ca	Displays the expanded client certificate (including PEM format) associated with the specified Map ID. If no client certificate has been imported this command displays a message to that effect. If no Map ID is specified, all client certificates are displayed. **Syntax**: `Intel 7115> show client_ca <mapID>` where <mapID> is the mapID number of the key whose imported client certificate you wish to display.

Command	Description
import client_ca	If you wish to authenticate a client, use this command to import the trusted CA's certificate. When enabled, clients without certificates or with invalid certificates are refused connection. **Syntax**: `Intel 7115> import client_ca <mapID>` `Import protocol: (paste, xmodem, uudecode) [paste]: <Enter>` `Type or paste in data, end with ... alone on line` (certificate pasted here...) `...` where `<mapID>` is the mapID number with which the client certificate will be associated.
delete client_ca	Deletes the client certificate associated with the specified Map ID. **Syntax**: `Intel 7115> delete client_ca <mapID>` where `<mapID>` is the mapID number whose associated client certificate you wish to delete.
create sign	Create the signing request for a specified Key ID. **Syntax**: `Intel 7115> create sign <keyID>` where `<keyID>` is the Key ID number of the Key for which you wish to create a signing request.

Command	Description
delete sign	Delete the signing request for a specified Key ID. **Syntax**: `Intel 7115> delete sign <keyID>` where `<keyID>` is the Key ID number of the Key whose signing request you wish to delete.
export sign	Export signing request (PEM format) for specified Key ID. **Syntax**: `Intel 7115> export sign <keyID>` where `<keyID>` is the Key ID number of the Key whose signing request you wish to export.
show sign <keyID>	Display expanded signing request (PEM format) for specified Key ID. If no Key ID is specified, all signing requests are displayed. **Syntax**: `Intel 7115> show sign <keyID>` where `<keyID>` is the Key ID number of the key whose signing request you wish to display.

Command	Description
set defcert	Set the default certificate creation information. For example, country, state, city, organization, organization unit, issuer name, and issuer e-mail address. You can change all, some or none of the fields. Press **Enter** to accept a default and move to the next field. **Example**: `Intel 7115> set defcert` `Country name [US]:` `State [California]:` `City [San Diego]:` `Organization [Intel Corporation]:` `Organization unit [Network Equipment Division]:` `Issuer name [www.server.com]:` `Issuer email address [support@server.com]: email@server.com` `Make changes [y]: y` `Changes applied` `Intel 7115>`
show defcert	Display the default certificate creation information. **Example**: `Intel 7115> show defcert` `Country: US` `State: California` `City: San Diego` `Organization: Intel Corporation` `Unit: Network Equipment Division` `Name: http://www.intel.com/network/services` `Email: email@server.com` `Intel 7115>`

Command	Description
set kstrength	Set the default key strength. Usable values are 512 or 1024. The default value is 512. **Syntax**: `Intel 7115> set kstrength <512 | 1024>` where <512> allows you to specify low key strength and <1024> allows you to specify high key strength.
show kstrength	Display the default key strength value. **Example**: `Intel 7115> show kstrength` `Default key strength: 512`
set client_tmo	Interval that the connection between the client and server can remain idle (i.e., no data crosses the connection in either direction) following a client request. **Syntax**: `Intel 7115> set client_tmo <n>` where <n> is a value in seconds between 5 and 36000.
show client_tmo	Displays the currently specified client timeout value. **Example**: `Intel 7115> show client_tmo` `Client timeout is 5 seconds` `Intel 7115>`

Command	Description
set server_tmo	Limits the period of time to establish a connection with the server. If the connection is not established within the specified time, the client request is rejected. ***NOTE:*** *Typical causes for server timeout include: server powered off, server not accessible, application is not available on the specified port.* **Syntax**: `Intel 7115> set server_tmo <n>` where <n> is a value in seconds between 5 and 36000.
show server_tmo	Displays the currently specified server timeout value. **Example**: `Intel 7115> show server_tmo` `Server timeout [secs]: 5` `Intel 7115>`

Port Mapping Commands

These commands are used to execute the operations described in Chapter 3's *Mapping* and *Blocking* sections.

Command	Definition
create block	Create a block to preclude access to specified IP addresses or through specified ports. A single IP, a single port, or all ports can be blocked. If fewer than all ports are to be blocked, you must repeat the **create block** command for each one. **Example**: `Intel 7115> create block` `Client IP to block [0.0.0.0]: 10.1.2.1` `Client IP mask [0.0.0.0]: 255.255.0.0` `Server IP to block [0.0.0.0]: 20.1.2.1` `Server IP mask [0.0.0.0]: 255.255.0.0` `Server Port to block: 80` `Server Port mask [0xffff]:<Enter>` `Intel 7115>`
delete block	Delete a block specified by index number. Use **show block** (see below) to correlate existing blocks with their numbers. **Example**: `Intel 7115> delete block 1` `Intel 7115>`
show block	Display all existing blocks. **Example**: `Intel 7115> show block` `--------` `blocks :` `---------` `(1) block 10.1.2.1 255.255.0.0 20.1.2.1 255.255.0.0 80 0xffff` `----------`

Command	Definition
create permit	Create a configuration allowing a specified user access to specified servers and ports, and/or denying the specified user access to specified servers and ports. **Example**: `Intel 7115> create permit` `Client IP to permit [0.0.0.0]:10.1.2.1` `Client IP mask [0.0.0.0]:255.255.0.0` `Server IP to permit [0.0.0.0]:20.1.2.1` `Server IP mask [0.0.0.0]:255.255.0.0` `Server Port to permit: 443` `Server Port mask [0xffff]:<Enter>` `Intel 7115>`
delete permit	Delete a permit specified by index number. Use **show permit** (see below) to correlate existing permits with their numbers. **Example**: `Intel 7115> delete permit 1` `Intel 7115>`
show permit	Display permits currently in force. **Example**: `Intel 7115> show permit` `--------` `permits :` `---------` `(1) permit 10.1.2.1 255.255.0.0 20.1.2.1 255.255.0.0 443 0xffff` `----------` `Intel 7115>`

Command	Definition
create map	Create a mapping that associates server IP, SSL port, clear text port, and Key ID. **Example**: `Intel 7115> create map` `Server IP (0.0.0.0): 1.1.1.1` `SSL (network) port [443]: 443` `Cleartext (server) port [80]: 8080` `KeyID to use for mapping: 4` `Intel 7115>` ***NOTE:*** *The Key ID used with a new mapping must exist prior to executing* ***create map****. Use* ***create key*** *to create a new Key ID. Also, a certificate must be associated with the key ID prior to using the mapping. (See Chapter 3 for details.)*
delete map <mapID>	Delete a mapping. ***NOTE:*** *All MapIDs of a higher number than the one specified for deletion are decremented by one when this command is executed.* **Syntax**: `Intel 7115> delete map <n>` where <n> is the Map ID of the mapping you wish to delete.
show map	Display all mappings. (Same as **list maps**.)
list maps	List all mappings. (Same as **show map**.) **Example**: `Intel 7115> list maps` `Map Net Ser Cipher Re- Client` `ID KeyID Server IP Port Port Suites direct Auth` `== ===== ========= ==== ==== ====== ===== ====` `1 default Any 443 80 all(v2+v3) n n` `2 sample 1.1.2.5 443 80 med(v2+v3) n n` `Intel 7115>`

Operational Commands

Command	Description
bypass ***WARNING:*** *Do not issue the* ***bypass*** *command from a remote management session (Telnet or SSh). Doing so will result in an immediate disconnect from the 7110/7115.*	Enables bypass mode, in which traffic flows through 7110/7115 without being processed. See *Failure/Bypass Modes* in Appendix B for details. See the **inline** command below for reversing bypass. **Example**: `Intel 7115> bypass` The LED labeled "inline" on the 7110/7115's front panel turns off when bypass is enabled. ***NOTE:*** *The 7110/7115 can be placed in bypass mode simultaneously with the bypass switch and the CLI's* ***bypass*** *command. When this occurs, you must use both the bypass switch and the CLI's* ***insert*** *command to return the unit to inline mode.*
inline	Enables inline mode, in which the 7110/7115 processes traffic normally. (As opposed to bypass mode, in which traffic may flow through the device unprocessed.) **Example**: `Intel 7115> inline` The LED labeled "inline" on the 7110/7115's front panel is illuminated when inline mode is enabled. ***NOTE:*** *Other factors may preclude the use of inline mode. See* Failure/Bypass Modes *in Appendix B.*

Command	Description
set spill	Allows you to enable or disable spill mode. "Spill" is used to offload processing of a request, when the 7115 has reached a specified queue threshold, to a secondary 7115 or to the server. **Example**: `Intel 7115> set spill enable` Verify spill setting with the **show spill** command: `Intel 7115> show spill` `Spill on overload: enabled` `Intel 7115>`
show spill	Display spill setting (enabled or disabled). **Example**: `Intel 7115> show spill` `Spill on overload: disabled`
reboot	Reboots the 7115. ***WARNING:*** *Any configuration changes mede during the current CLI session will be lost upon rebooting. Refer to the* ***config save*** *command for details regarding saving configuration changes.* **Example**: `Intel 7115> reboot` `Are you sure you want to reboot [n]: y` `System rebooting...done` (System reboots, eventually prompting you for your password.)

Remote Management Commands

Command	Description
set ip	Assign an IP address and netmask to the 7115's network interface for Telnet and SSh sessions. ***CAUTION:*** *The assignment of an IP address introduces security issues. Please refer to the "Access Control" section of Chapter 6.* ***NOTE:*** *To disable a currently configured IP, use* ***set ip*** *followed by* ***none****.* **Example:** `Intel 7115> set ip` `Enter IP Address ('none' to delete)` `[10.1.2.124]:` `Enter Netmask [255.255.0.0]:`
set max_remote_sessions	Set the maximum allowed number of concurrently running Telnet and SSh sessions. **Syntax:** `Intel 7115> set max_remote_sessions <1-5>` where `<1-5>` is the maximum number of remote sessions you wish to allow. Default: 5.

Command	Description
set telnet	Enables or disables Telnet sessions. When this command is set to "enable" and an IP address is assigned to the 7115's network interface, you can access the device's CLI via remote Telnet session. When disabled, the device refuses Telnet connections. The console prompts for any missing parameters. Default: disable. **Syntax:** `Intel 7115>` **`set telnet enable`** `Need an IP address to start Telnet service.` `Enter IP Address [209.218.240.67]:` **`10.1.2.124`** `Need a netmask to start Telnet service.` `Enter Netmask [255.255.255.0]:` `Optional Default Route to start Telnet service.` `Enter Default Route ('none' to delete) [none]:` `Telnet Services started.` `Intel 7115>`
show telnet	Displays current telnet status: enabled or disabled. **Example:** `Intel 7115>` **`show telnet`** `Telnet: Enabled`
set telnet_port	Set the port on which Telnet connections are accepted. (Default port: 23.) **Syntax:** `Intel 7115>` **`set telnet_port <port>`** where `<port>` is the number of the port to which Telnet sessions will connect.

Command	Description
show telnet_port	Display the port on which Telnet sessions are currently accepted. **Example:** `Intel 7115> show telnet_port` `Telnet port: 23`
set ssh	Enable or disable Secure Shell (SSh) sessions. When this command is set to "enable" and an IP address is assigned to the 7115's network interface, you can access the device's CLI via remote SSh session. When disabled, the device refuses SSh connections. Default: disable. **Syntax:** `Intel 7115> set ssh <enable|disable>`
show ssh	Display current SSh status: enabled or disabled. **Example:** `Intel 7115> show ssh` `SSH: Disabled`
set ssh_port	Set the port on which SSh connections are accepted. (Default port: 22.) **Syntax:** `Intel 7115> set ssh_port <port>` where `<port>` is the number of the port to which SSh sessions will connect.
show ssh_port	Display port on which SSh sessions are currently accepted. **Example:** `Intel 7115> show ssh_port` `SSH port: 22.`

Command	Description
setsnmp snmp	Enable or disable the SNMP agent. When enabled, you can set configure SNMP information and parameters (see **setsnmp snmp_info**, below) for the 7115. Default: disable. **Syntax:** `Intel 7115> setsnmp <enable|disable>`
showsnmp snmp	Displays the current status of the SNMP agent: enabled or disabled. **Example:** `Intel 7115> showsnmp snmp` `SNMP: Enabled`
setsnmp snmp_info	Set the following SNMP information and parameters: • SNMP port (Default: 161) • SNMP trap port (Default: 162) • Contact person • System name • System location **Example:** `Intel 7115> setsnmp snmp_info` `SNMP port [161]: 161` `SNMP trap port [162]: 162` `Contact Person []: support` `System Name []: 7115` `System Location []:San Diego`

Command	Description
showsnmp snmp_info	Display the currently effective SNMP information and parameters. **Example:** `Intel 7115> showsnmp snmp_info` `SNMP Port Number : 161` `SNMP Trap Port Number: 162` `SNMP System Contact : support` `SNMP System Name : 7115` `SNMP System Location : San Diego` `System IP Address : 10.1.2.124` `System Netmask : 255.255.255.0` `Default Route : None`
setsnmp snmp_community	Set SNMP community strings. **Example:** `Intel 7115> setsnmp snmp_community` `IP []:xxx.xxx.xxx.xxx` `Community String []:<string>`
list snmp_community	Display currently configured SNMP community strings. **Example:** `Intel 7115> list snmp_community` `<2> Current Available SNMP Community String(s):` `1.) IP: 0.0.0.0 => String: public` `2.) IP: 0.0.0.0 => String: private`
delete snmp_community	Delete SNMP community strings. **Example:** `Intel 7115> delete snmp_commmunity` `SNMP Community String(s) Deletion.` `<2> Current Available SNMP Community String(s):` `1.) IP: 0.0.0.0 => String: public` `2.) IP: 0.0.0.0 => String: private` `Enter number (1 to 2) to delete (q to quit) [1]: 2` `Enter number (1 to 2) to delete (q to quit) [1]: q`

Command	Description
setsnmp trap_authen	When enabled, the SNMP manager receives traps upon failed authentication attempts. **Example**: `Intel 7115> setsnmp trap_authen <enable|disable>`
setsnmp trap_authen	Displays current status of trap authentication trap. **Example:** `Intel 7115> showsnmp trap_authen` `Trap Authentication: Enabled`
setsnmp trap_community	Sets SNMP trap community strings. **Example:** `Intel 7115> setsnmp trap_community` `SNMP Trap Community String(s) Setting.` `Enter a SNMP Trap Community IP (q to quit): 0.0.0.0` `Enter a SNMP Trap Community String (q to quit): private` `Enter a SNMP Trap Community IP (q to quit): 0.0.0.0` `Enter a SNMP Trap Community String (q to quit): public` `Enter a SNMP Trap Community IP (q to quit): q`
list trap_community	Display SNMP trap community strings. **Example:** `Intel 7115> list trap_community` `SNMP Trap Community String(s) information.` `<2> Current SNMP Trap Community String(s):` `1.) IP: 0.0.0.0 => String: public` `2.) IP: 0.0.0.0 => String: private`

Command	Description
delete trap_community	Delete SNMP trap community strings. **Example:** `Intel 7115>` **`delete trap_community`** `SNMP Trap Community String(s) Deletion.` `<2> Current Available SNMP Trap Community String(s):` `1.) IP: 0.0.0.0 => String: public` `2.) IP: 0.0.0.0 => String: private` `Enter number (1 to 2) to delete (q to quit) [1]:` **`2`** `Enter number (1 to 2) to delete (q to quit) [1]:` **`q`**

Alarms and Monitoring Commands

Command	Description
set alarms	Enable all or a selection of the 7115's alarms. **Syntax:** `Intel 7115> set alarms <all|esc|rsc|utl|ovl|nls>` where <all> enables all five of the 7115's alarms. <esc> enables the Encryption Status Change Alarm. <rsc> enables the Refused SSL Connection Alarm <utl> enables the Utilization Threshold Alarm <ovl> enables the Overload Alarm <nls> enables the Network Link Status Alarm To disable all alarms, use **none**: **Example:** `Intel 7115> set alarms all` `Intel 7115> show alarms` `Alarms set: esc rsc utl ovl nls`
show alarms	Display the list of currently enabled alarms. **Example:** `Intel 7115> set alarms none` `Intel 7115> show alarms` `Alarms set:` ***NOTE:*** *When no alarms are set (i.e., when **none** is specified in **set alarms**), the display shows an empty field.*
set rsc_window	Set interval (window) at which the device checks for refused SSL connections and, if any are detected, issues an RSC Alarm. (Range: 5-65000 seconds, default: 15) **Syntax:** `Intel 7115> set rsc_window <sec>` where <sec> is the number of seconds of the desired interval.

Command	Description
show rsc_window	Display current Refused SSL Connections Alarm interval. **Syntax:** `Intel 7115> show rsc_window` `Check refused SSL connections [secs]: 10`
set utl_window	Set interval (window) at which the device checks for exceeded utilization thresholds (CPU load, Connections per Second, or Total Open Connections and, if any are detected, issues a Utilization Threshold Alarm. (Range: 5-65000 seconds, default: 15) ***NOTE:*** *The data collected for utilization threshold metrics tends to be bursty,so a smoothing algorithm is used to prevent continuous alarms.The utilization window is a user-specified sliding interval during which data is collected and averaged. Consequently, shorter intervals are likely to result in some extraneous alarms.* ***NOTE:*** *See also* ***set utl_highwater*** *and* ***set utl_lowwater****, this section.* **Syntax:** `Intel 7115> set utl_window <sec>` where <sec> is the number of seconds of the desired interval.
set utl_highwater	Set the Utilization Threshold Alarm high-water value. Expressed as a percentage, the high-water value represents the highest CPU utilization, Connections per Second, or Total Open Connections required to trigger a UTL Alarm. (Range: 2-100%, default: 90) ***NOTE:*** *See also* ***set utl_window*** *and* ***set utl_lowwater****, this section.* **Syntax:** `Intel 7115> set utl_highwater <%>` where <%> is the percentage defining the upper threshold of CPU utilization, Connections per Second, or Total Open Connections required to trigger a Utilization Threshold Alarm.

Command	Description
set utl_lowwater	Set the Utilization Threshold Alarm low-water value. Expressed as a percentage, the low-water value represents the lowest CPU utilization, Connections per Second, or Total Open Connections required to trigger a UTL Alarm. (Range: 2-100, default: 90) ***NOTE:*** *See also* ***set utl_window*** *and* ***set utl_highwater****, this section.* **Syntax:** `Intel 7115> set utl_lowwater <%>` where <%> is the percentage defining the lower threshold of CPU utilization, Connections per Second, or Total Open Connections required to trigger a Utilization Threshold Alarm.
show utl_window	Display the current Utilization Threshold Alarm window. **Example:** `Intel 7115> show utl_window` `Utilization window set [secs]: 10.`
show utl_highwater	Display the Utilization Threshold Alarm's current upper threshold. **Example:** `Intel 7115> show utl_highwater` `Utilization High water mark [%]: 80`
show utl_lowwater	Display the Utilization Threshold Alarm's current lower threshold. **Example:** `Intel 7115> show utl_lowwater` `Utilization Low water mark [%]: 60`
set ovl_window	Set interval (window) at which the device checks for overloads resulting in the device executing a spill or throttle and, if any are detected, issues an Overload Alarm. (Range: 5-65000, default: 15) **Syntax:** `Intel 7115> set ovl_window 10`

Command	Description
show ovl_window	Display the current Overload Alarm window. **Example:** `Intel 7115> show ovl_window` `Check for overload conditions [sec]: 10`

Configuration Commands

Command	Description
show config	Display current volatile configuration settings. **Example**: `Intel 7115> show config` `# default config file created on Tues July 25 06:56:46 2000` *(Configuraton parameters are displayed here...)* `Intel 7115>`
show config saved	Display saved non-volatile configuration settings. **Example**: `Intel 7115> show config saved` `Saved configuration` `==========` *(Configuraton parameters are displayed here...)* `Intel 7115>`

Command	Description
show config default	Display default configuration settings. These are values used when factory default commands are executed. **Example**: `Intel 7115> show config default` `Default configuration` `==========` `conlog 0xfffffef` `ilog 0xffffffff` `trace 0xfffff3dd` `media auto` `logport tty01` `cache 3` `server_tmo 5` `client_tmo 30` `serverif exp1` `netif exp0` `map 0.0.0.0 443 80 default` `kpanic reboot` `monitoring_interval 15` `monitoring_fields 0x1F` `alarm_mask 0x00000000` `ovl_window 15` `rsc_window 15` `utl_window 15` `utl_high 90` `utl_low 60` `idle 300` `kstrength 512` `con_speed 9600` `con_bits 8` `con_stop 1` `con_parity n` `max_remote_sessions 5` `trap_authen 1` `defcert_cname US` `defcert_state California` `defcert_city San Diego` `defcert_orgname Intel Corporation` `defcert_orgunit Network Equipment Division` `defcert_name www.intel.com` `defcert_email support@intel.com` `prompt Intel 7115>` `Intel 7115>`

Command	Description
config compare	Display differences between saved and current configuration. For optimal flexibility in configuration and testing, the 7115 supports both "current" (volatile) and "saved" (non-volatile) configurations. The config compare command displays the differences, if any, between the two configurations. **Example**: `Intel 7115> config compare` `Only in /keys: 4` `Intel 7115>`
config reset	Restore saved configuration (no reboot). **Example**: `Intel 7115> config reset` `Reverting to saved configuration` `Reset (y/n) [n]: n` `Intel 7115>`
config default	Clears current and saved configurations and restores factory defaults. ***WARNING:*** *Executing this command causes the system to reboot.* **Example**: `Intel 7115> config default` `Reset to factory default configuration [n]: y` `Reset to factory defaults` `System rebooting...`
config save	Save the current configuration to the flash (non-volatile) memory. **Example**: `Intel 7115> config save` `Saving configuration to flash...` `Configuration saved to flash` `Intel 7115>`

Command	Description
export config ***WARNING:*** *Do not edit an exported configuration file.*	Export all configuration, key, sign and certificate information (ASCII, xmodem, uuencode). **Example**: `Intel 7115> export config` `Export protocol: (xmodem, uuencode, ascii) [ascii]:` `Press any key to start, then again when done...` `# default config file created on Fri Jul 28 06:56:46 2000` (...configuration specifics are displayed...) `Intel 7115>`
import config	Import a configuration file (paste, xmodem, uudecode). **Example**: `Intel 7115> import config` `Import protocol: (paste, xmodem) [paste]:` `Type or paste in data, end with ... alone on line` `.` `.` `.` `Do you want to install this config ? [y]: n` `Intel 7115>`

Command	Description
import upgrade	Import a complete software release. (See Chapter 6 for details regarding software updates.) **Example**: `Intel 7115> import upgrade` `Import protocol: (xmodem, uudecode)` `[xmodem]:` `Start xmodem upload now` `Use Ctl-x to cancel upload` `Verifying upgrade image...` `upgrade image valid` `version x.x, build xxx` `Continue with the upgrade? [n]:y` ***NOTE:*** *Note, all save logs will be deleted and the system will reboot upon sucessful completion of the upgrade*
import patch	Import a partial software upgrade **Example:** `Intel 7115> import patch` `Enter patch name [80.patch] <patch name>` `Import protocol: (xmodem, uudecode)` `[xmodem]:` `Start xmodem upload now` `Use Ctl-x to cancel upload` `Patch: Imported.`
list system	Displays the device's CPU, memory and crypto card information. `Intel 7115> list system` `================================================` `SYSTEM INFO` `================================================` `* CPU : Pentium II (498 MHz) GenuineIntel` `* Real MEM : 536870912 (512.00 MB)` `* Crypto : 3`

Command	Description
factory_default	Returns to factory configuration settings. **Example**: `Intel 7115> factory_default` `Reset to default configuration [n]: y` `Reset to factory defaults` `System rebooting...done` `T944 V2.31 DXC.` `..` `868242+3611880/S running` `Generating 512 bit default key` `Generating default certificate` `Saving default key/cert to flash` `Restricted Rights Legend` *(...copyright and version information displayed here...)* `Serial 0:a0:a5:11:4:9d` `password:`

Administration Commands

Command	Description
password	Set the password. **Example**: `Intel 7115> password` `Old password:<xxxxx>` `Enter new admin password (5 chars min.):<yyyyy>` `Retype new password:<yyyyy>` `admin Password changed...` `Intel 7115>`
show info	Display software version information. **Example**: `Intel 7115> show info` `==========` `=== Intel(R) NetStructure(tm) 7115` `e-Commerce Accelerator` `=== Copyright (c) 2000 Intel Corporation` `=== All rights reserved.` `===` `=== Version 2.3, Build xxx` `==========`
set date	Set the date and time. ***WARNING:*** *Execution of this command reboots the 7115.* **Example**: `Intel 7115> set date` `Year [2000]:` `Month [2]:` `Day [16]:` `Hour (24 hour clock) [15]:` `Minute [10]:` `The system must reboot for changes to take affect. Reboot [y]: n` `Intel 7115>`
show date	Displays current date and time.

Command	Description
set egress_mac	Allows the configuration of a 7115 when the ingress and egress traffic paths are different. (See Chapter 4, Scenario 4.)
set ether	Specify ethernet settings. **Example**: `Intel 7115> set ether` `1 - auto` `2 - 10baseT, half duplex` `3 - 10baseT, full duplex` `4 - 100baseTX, half duplex` `5 - 100baseTX, full duplex` `Select media type [1]:` `Media set to auto` `Intel 7115>`
show ether	Display ethernet settings. **Example**: `Intel 7115> show ether` `Ethernet media set to auto` `Intel 7115>`
set idleto	Set the console idle interval. After <n > minutes absence of keyboard activity, the user is automatically logged off. **Syntax**: `Intel 7115> set idleto <n>` where <n> is a value in minutes.
show idleto	Display console timeout. **Example**: `Intel 7115> show idleto` `Idle timeout is 5 minutes` `Intel 7115>`

Command	Description
set more	Set the page length of the console display. Default is 300. **Syntax**: `Intel 7115> set more <n>` where <n> is the desired number of lines. Valid inputs are 0 (to disable), or 23 or greater.
nic	Allows you to set the network interface card configuration. **Example**: `Intel 7115> nic` `1 - auto` `2 - 10baseT, half duplex` `3 - 10baseT, full duplex` `4 - 100baseTX, half duplex` `5 - 100baseTX, full duplex` `Select media type [1]:`
set prompt	Change the prompt from `Intel 7115>` to the desired prompt. **Example**: `Intel 7115> set prompt` `Prompt [Intel 7115> ]: <Enter>` `Intel 7115>`
set serial	Allows user to set the console port to monitor the CLI or the output logging, and set the speed, data bits, stop bits, and parity bits. The aux console port is fixed at 115200, 8, 1, N. This command returns the user to the "password" prompt after setting the console port. **Example**: `Intel 7115> set serial` `Baud rate (9600/115200) [9600]: <Enter>` `Data bits (7/8) [8]: <Enter>` `Stop bits (1/2) [1]: <Enter>` `Parity (n/e/o) [n]: <Enter>` `Set serial parameters [y]: <Enter>` `Intel 7115>`

Command	Description
show serial	Display console serial parameters. **Example**: `Intel 7115> show serial` `Speed: 9600` `Bits: 8` `Stop bits: 1` `Parity: n` `Intel 7115>`
exit	Log the user out of the CLI. If the current configuration has changed, the user is allowed to save the current configuration as the active configuration. **Example**: `Intel 7115> exit` `Goodbye` `.` `.` `.` `password:`

Logging Commands

Command	Description
export log ***NOTE:*** *Log files referred to here are not human-readable.*	Export a saved log/trace file. **Syntax**: `Intel 7115> export log <logID>` where `<logID>` is the ID of the specific log you wish to export. **Example**: `Intel 7115> export log a` `Export protocol: (xmodem, uuencode)` `[xmodem]:` `Use Ctrl-X to kill transmission` `Beginning export...`

Command	Description
delete log	Delete saved log/trace files from /flash/logs. **Syntax**: `Intel 7115> delete log <logID> | all` where `<logID>` is the ID of the specific log you wish to delete, and `all` deletes all logs.
list logs	List all log files.

6 Remote Management

Overview

The current software release allows you to remotely manage the 7110/7115. Remote management is available via three protocols:

- Telnet
- Secure Shell (SSh)
- SNMP

NOTE: *Remote management functions can be enabled and configured only through the local serial console.*

When enabled, remote management allows you to access the device's Command Line Interface (CLI) from Telnet or SSh sessions running on remotely located machines. Up to five remote sessions can be configured, including both Telnet and SSh sessions (Default: 5). Before you can use the device's remote management function, you must enable and configure it at the local serial console. Remote management requires that the device's network interface be assigned an IP address, unlike earlier versions of the 7110.

Remote SNMP management is supported to the extent of allowing control of the System group of MIB-II.

Limitations

Note that several CLI capabilities available at the local console are unavailable in remote sessions. These are:

- Assignment of an IP address to the 7110/7115's network interface
- Enable/disable Telnet, SSh, or SNMP
- Change Telnet, SSh, or SNMP ports
- Set maximum number of Telnet or SSh sessions
- Enable/disable monitoring report or alarms (Though reports and alarms can be received remotely when these features are enabled at the serial console prior to enabling remote management.)

The CLI commands that control remote management potentially affect the device's configuration files, thus if a remote management configuration is to persist across a shutdown/startup of the device, you must follow remote management configuration with the CLI command **config save**. This ensures that the configuration will be restored upon startup.

Remote Management CLI Commands

Remote management is enabled or disabled and configured by using a series of CLI commands available only at the local serial console. The exact sequence varies depending on the type and configuration of the remote session you wish to enable. (Usage is detailed in subsequent sections.) These commands are:

General:

- **set ip <ip> <netmask>** assigns an IP address and netmask to the 7110/7115's network interface.
- **set max_remote_sessions <1-5>** sets the maximum allowed number of concurrently running Telnet and SSh sessions.

Telnet-specific:

- **set telnet enable|disable** enables or disables Telnet sessions.
- **show telnet** displays current telnet status: enabled or disabled.
- **set telnet_port <port>** sets the Telnet port. (Default: 23.)

- **show telnet_port** displays current telnet port.

  SSh-specific:

- **set ssh enable|disable** enables or disables SSh sessions.
- **show ssh** displays current SSh status: enabled or disabled.
- **set ssh_port <port>** sets the SSh port. (Default: 22.)
- **show ssh_port** displays current SSh port.

  SNMP-specific:

- **setsnmp snmp enable|disable** enables or disables SNMP management.
- **showsnmp snmp** displays current SNMP status: enabled or disabled.
- **setsnmp snmp_info** sets the following SNMP information and parameters:
  - SNMP port (Default: 161)
  - SNMP trap port (Default: 162)
  - SNMP agent IP address
  - Contact person
  - System name
  - System location
- **showsnmp snmp_info** displays current SNMP information and parameters.
- **setsnmp snmp_community** sets SNMP community strings.
- **list snmp_community** displays SNMP community strings.
- **delete snmp_community** deletes SNMP community strings.
- **setsnmp trap_community** sets SNMP permission strings.
- **list trap_community** displays SNMP permission strings.
- **delete trap_community** deletes SNMP permission strings.

Remote Telnet Sessions

This section contains procedures for accessing the 7110/7115's CLI via remote Telnet session.

Local Serial Console

Assign an IP address to the 7110/7115's network interface using the following procedure:

```
Intel 7115> set ip
Enter IP [10.1.2.56]: 10.1.1.1
Enter Netmask [255.255.255.0]:
```

Verify the IP and netmask (optional):

```
Intel 7115> show ip
System IP Address : None
System Netmask    : None
Intel 7115>
```

Enable remote Telnet sessions:

```
Intel 7115> set telnet enable
```

Configure the network route:

```
Intel 7115> set route
Enter Default Route ('none' to delete)
[10.1.1.1] : <enter>
```

Verify the route configuration (optional):

```
Intel 7115> show route
Default Route : 10.1.1.1
```

Delete a route configuration (optional):

```
Intel 7115> set route none
```

NOTE: *To ensure that this remote management configuration persists across a device shutdown and startup, run the* ***config save*** *command.*

Remote Telnet management is now enabled and configured on the 7110/7115. Now you can access the CLI from a remote Telnet session.

Remote Console, Telnet

With remote Telnet enabled on the 7110/7115, use the following procedure to access it's CLI:

```
Unix-prompt> telnet 10.1.1.1
Trying 10.1.1.1...
Connected to 10.1.1.1.
Escape character is '^]'.

.

.

.

Serial 0:a0:a5:11:4:2e
password:<password>
```

*NOTE: If other remote sessions are already running and the new one exceeds the number allowed as configured with the **set max_remote_sessions** command, the CLI displays the message, "Max Remote Sesion Limit of (5) exceeded!" Either close a session, or increase the maximum number allowed.*

After you enter your password, the Telnet session displays the 7110/7115's CLI. From this point, you can manage the device as you would from the local serial console, minus the few disallowed commands listed in the "Limitations" section near the beginning of this chapter.

Changing the Telnet Port

The Telnet port is set and displayed by using the CLI commands, **set telnet_port <port>** and **show telnet_port**.

These commands are available only at the local serial console and when the remote management is enabled. By default, the Telnet port number is 23.

To set the Telnet port:

```
Intel 7115> set telnet_port 230
```

To display the Telnet port:

```
Intel 7115> show telnet_port
Telnet Port Number: 230
```

Disabling Telnet

Telnet sessions are disabled at the 7110/7115's local serial console. To disable, follow the steps below:

```
Intel 7115> set telnet disable
```

To verify Telnet disable:

```
Intel 7115> show telnet
Telnet: disable
```

To ensure that Telnet sessions remain disabled across a device shutdown and startup, run the **config save** command.

Remote SSh Sessions

This section contains procedures for accessing the 7110/7115's CLI via remote Secure Shell (SSh) session.

Local Serial Console

Assign an IP address to the 7110/7115's network interface using the following procedure:

```
Intel 7115> set ip
Enter IP [10.1.2.56]: 10.1.1.1
Enter Netmask [255.255.255.0]:
```

Verify the IP and netmask (optional):

```
Intel 7115> show ip
System IP Address: 10.1.1.1
System Netmask: 255.255.255.0.
```

Enable remote SSh sessions:

```
Intel 7115> set ssh enable
```

Configure the network route:

```
Intel 7115> set route
Enter Default Route ('none' to delete)
[10.1.1.1] : <enter>
```

Verify the route configuration (optional):

```
Intel 7115> show route
Default Route : 10.1.1.1
```

Delete a route configuration (optional):

```
Intel 7115> set route none
```

*NOTE: To ensure that this remote management configuration persists across a device shutdown and startup, run the **config save** command.*

Remote SSh management is now enabled and configured on the 7110/7115. Now you can access the CLI from a remote SSh session.

Remote Console, SSh

With remote SSh enabled on the 7110/7115, use the following procedure to access it's CLI:

```
Unix-prompt> ssh -1 admin 10.1.1.1

.
.
.

Serial 0:a0:a5:11:4:2e

password:<password>
```

*NOTE: If other remote sessions are already running and the new one exceeds the number allowed as configured with the **set max_remote_sessions** command, the CLI displays the message, "Max Remote Sesion Limit of (5) exceeded!" Either close a session, or increase the maximum number allowed.*

After you enter your password, the SSh session displays the 7110/7115's CLI. From this point, you can manage the device as you would from the local serial console, minus the few disallowed commands listed in the "Limitations" section near the beginning of this chapter.

Changing the SSh Port

The SSh port is set and displayed by using the CLI commands, **set ssh_port <port>** and **show ssh_port**.

These commands are available only at the local serial console and when the remote management is enabled. By default, the SSh port number is 22.

To set the SSh port:

```
Intel 7115> set ssh_port 220
```

To display the SSh port:

```
Intel 7115> show ssh_port
SSH Port Number: 220
```

Disabling SSh

SSh sessions are disabled at the 7110/7115's local serial console. To disable, follow the steps below:

```
Intel 7115> set ssh disable
```

To verify SSh disable:

```
Intel 7115> show ssh
SSH: disable
```

To ensure that SSh sessions remain disabled across a device shutdown and startup, run the **config save** command.

SNMP

The Intel® NetStructure™ 7110/7115 e-Commerce Accelerator has a fully compliant, embedded SNMP agent that supports SNMPv1 and SNMPv2 requests. In addition to standard MIB-II, Intel private enterprise MIBs provide the following capabilities:

- Monitor the health of the 7110/7115's hardware and network links
- Monitor the flags used to enable and disable alarms and monitors
- Monitor the 7110/7115's load as indicated by CPU utilization, connection count, and connections per second
- Monitor status and performance of SSL encryption and decryption functions
- Monitor overloads, spills, and throttles

Standards Compliance

The 7110/7115 SNMP agent is bilingual and can support both SNMPv1 and SNMPv2c requests. Intel private enterprise MIB files are compliant with SMIv2 as specified in RFC 1902. SET operations are not allowed for any Intel private MIB objects for the 7110/7115, although you can change MIB variable values by way of commands issued on the CLI.

Intel MIB Tree

Figure 6-1 illustrates the top level of Intel's MIB tree.

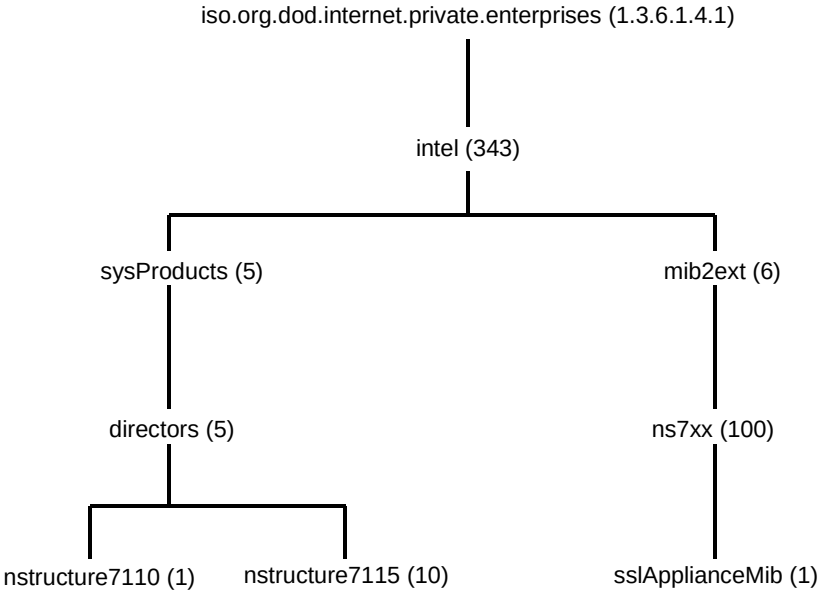

Figure 6-1: Intel's MIB Tree (top level)

All Intel enterprise MIBs and MIB objects are defined under the mib2ext branch of the `Intel` tree. All `sysObjectIds` that identify Intel products are defined under the `sysProducts` branch of the Intel tree.

Supported MIBs

Management Information Base-II (MIB-II)

Intel Enterprise MIBs:

```
ceo-header.my
ssl-appliance-mib.my
```

Where to find MIB Files

Electronic copies of the Intel MIB files used by the 7110/7115 are shipped with the product on CD-ROM.

Write access through SNMP SET is not allowed for any MIB variables or SNMP groups. An SNMP SET on any group returns an error.

The standard SNMP traps, `coldStart`, `warmStart`, `authenticationfailure`, `linkUp` and `linkDown` are supported.

ceo-header.my

`ceo-header.my` contains all the `sysObjectIds` defined for Intel® NetStructure™ products. All `sysObjectIds` are defined under the `sysProducts/directors` branch of the `intel` tree. This MIB file contains the following `sysObjectId` definitions for the following e-Commerce Accelerator products:

- 7110 {343, 5, 5, 1}
- 7115 {343, 5, 5, 10}

Enterprise Private MIB Summary

Following is a summary of the 7110/7115 private MIB:

`mode`

`inline(1): Device is configured to accelerate SSL traffic`

`bypass(2): Device is configured to pass through all SSL traffic`

`failMode`

`safe(1): Two ethernet segments fail open, stopping traffic`

`through(2): Two ethernet segments fail shorted, allowing traffic to continue`

`spillMode`

`throttle(1): Device will throttle SSL connections when utilization reaches 100%`

`spill(2): Device will spill SSL connections when utilization reaches 100%`

`sslSessionCache`

`enabled(1): SSL session caching is turned on`

`disabled(2): SSL session caching is turned off`

`restarts`

`Number of times the system has restarted`

`appLastRestart`

`The value of sysUpTime at the time the last restart of the application process happened`

`encryptionAlarm`

`enabled(1): Encryption status change alarm is turned on`

`disabled(2): Encryption status change alarm is turned off`

`sslConnectionAlarm`

`enabled(1): SSL connection alarm is turned on`

`disabled(2): SSL connection alarm is turned off`

thresholdAlarm

enabled(1): Threshold alarm is turned on

disabled(2): Threshold alarm is turned off

overloadAlarm

enabled(1): Overload alarm is turned on

disabled(2): overload alarm is turned off

linkStatusAlarm

enabled(1): Network link status alarm is turned on

disabled(2): Network link status alarm is turned off

encryptProcessingState

on(1): SSL processing on

off(2):SSL processing halted

encryptProcessingStateReason

normal(1): Normal

hardware(2): Change caused by hardware fault

consoleBypass(3): Bypass mode enabled at console

consoleInline(4): Inline mode enabled at console

frontPanelBypass(5): Bypass mode enabled at front panel

frontPanelInline(6): Inline mode enabled at front panel

serverInterfaceState

State of the server-side interface

networkInterfaceState

State of the network-side interface

utilWindow

Sliding window (in seconds) to calculate average connections, CPU utilization, and active connnection rates

cpuUtil

CPU utilization percentage (0-100)

cpuUtilNetwork

CPU utilization percentage processing network traffic (0-100)

cpuUtilProxy

CPU proxy utilization percentage (0-100)

cpuUtilHiWater

CPU utilization high water mark (2-100)

cpuUtilLoWater

CPU utilization low water msrk (1-99)

cpuUtilState

When CPU utilization exceeds the hi water mark, CPU utilization state is in alert and is not returned to normal until the lo water threshold is crossed

sslCps

SSL connections per second

sslCpsMaximum

Maximum SSL connection rate in connections per second since (re)start

sslCpsHiWater

SSL connections per second high water mark

sslCpsLoWater

SSL connections per second low water mark

sslCpsState

When SSL connections per second exceeds the hi water mark, sslCpsState is in alert and is not returned to normal until the lo water threshold is crossed

sslConnCnt

Current number of concurrent open SSL connections

sslConnCntMaximum

Maximum number of concurrent open SSL connections since (re)start

sslConnTotal

Total number of SSL connections processed

sslConnCntHiWater

Concurrent open SSL connection count high water mark

sslConnCntLoWater

Concurrent open SSL connection count low water mark

sslConnCntState

When concurrent open SSL connection count exceeds the hi water mark, sslConnCntState is in alert and is not returned to normal until the lo water threshold is crossed

encryptedBps

Encryption rate in bytes per second

encryptedBpsMaximum

Maximum encryption rate in bytes per second since (re)start

encryptedBytesTotalMb

Total number of megabytes of data encrypted

decryptedBps

Decryption rate in bytes per second

decryptedBpsMaximum

Maximum decryption rate in bytes per second since (re)start

decryptedBytesTotalMb

Total number of megabytes of data decrypted

sslOverloadInterval

The periodic interval (in seconds) used when counting the number of spilled or throttled SSL connections. If any SSLconnections were spilled or throttled in the lastsslOverloadInterval, a trap is generated. If sslOverloadInterval is 0, no trap is generated

throttlesPerSec

Number of throttles per second

throttlesPerSecMaximum

Maximum number of throttles per second since (re)start

throttlesTotal

Total number of throttles since (re)start throttles

Total number of throttles in the last sslOverloadInterval

spillsPerSec

Number of spills per second

spillsPerSecMaximum

Maximum number of spills per second since (re)start

spillsTotal

Total number of spills since (re)start

spills

Number of spills in the last sslOverloadInterval

refusedSslInterval

The periodic interval (in seconds) used when counting the number of refused SSL connections. If any SSL connections were refused in this time interval, a trap is generated.

cipherSuiteMismatch

Number of refused SSL connections in the last refusedSslInterval which are due to inability of the client and server to agree upon a cipher suite

clientCertAuthFail

Number of refused SSL connections in the last refusedSslInterval which are due to authentication failure of the client certificate

Trap Summary

The following list summarizes the traps generated by the 7110/7115. For details about a particular trap, please read the description of each MIB above, or read the documentation within the MIB file. Traps are generated by SNMP.

Standard SNMP Traps

```
coldStart
warmStart
authenticationFailure
linkUp
linkDown
```

Private Traps in ssl-appliance-mib.my

`encryptionStopped`

Alert issued whenever the device stops processing SSL traffic

`encryptionResumed`

Resumes processing traffic after having been stopped

`serverInterfaceStateChanged`

The server-side interface state changed

`networkInterfaceStateChanged`

The network-side interface state changed

`cpuUtilAlert`

The device has exceeded the CPU utilization high water threshold

`cpuUtilNormal`

CPU utilization back to normal levels

`sslCpsAlert`

The device has exceeded the SSL connections per second high water threshold

`sslCpsNormal`

The SSL connections per second processed by the device is back to normal levels

sslConnCntAlert

The device has exceeded the open SSL connection count high water threshold

sslConnCntNormal

The open SSL connection count of the device is back to normal levels

sslConnectionRefusedMismatch

SSL connections were refused in the past sslRefusedInterval due to cipher suite negotiation

failuresslConnectionRefusedAuthFail

SSL connections were refused in the past sslRefusedInterval due to authentication failure of the client certificate

sslOverloadSpills

SSL connections were spilled in the past sslOverloadInterval

sslOverloadThrottles

SSL connections were throttled in the past sslOverloadInterval

appRestartAlert

SSL processing application has restarted

Enabling SNMP.

Enabling and disabling SNMP is accomplished with the CLI command, **setsnmp snmp enable|disable**. Operational status can be verified using **showsnmp snmp**.

Examples:

```
Intel 7115> setsnmp snmp enable

Intel 7115> showsnmp snmp
SNMP: enable

Intel 7115> setsnmp snmp disable

Intel 7115> showsnmp snmp
SNMP: disable
```

Specifying SNMP Information

Configurable SNMP parameters can be set collectively using the **setsnmp snmp_info** command as illustrated below:

```
Intel 7115> setsnmp snmp_info
SNMP port [161]: 161
SNMP trap port [162]: 162
Contact Person []: support
System Location []:
System Name []: 7115
```

Current values of SNMP parameters are displayed using the **shownmp snmp_info** command:

```
Intel 7115> showsnmp snmp_info
SNMP port: 161
SNMP trap port: 162
Contact Person: support
System Name: 7115
System IP Address: x.x.x.x
System Netmask: y.y.y.y
Default Route: z.z.z.z
```

You can also configure SNMP information elements individually using the following commands:

- **setsnmp snmp_port** sets the SNMP port
- **setsnmp trap_port** sets the SNMP trap port
- **setsnmp sys_contact** sets the contact person
- **setsnmp sys_name** sets the system name
- **setsnmp sys_location** sets the system location

Correspondingly, the values set with the above commands are displayed using the commands:

- **showsnmp snmp_port**
- **showsnmp trap_port**
- **showsnmp sys_contact**
- **showsnmp sys_name**
- **showsnmp sys_location**.

Community String

Use CLI commands **setsnmp snmp_community**, **list snmp_community** and **delete snmp_community** to set, list, and delete SNMP community strings.

```
Intel 7115> setsnmp snmp_community
IP []:
Community String []:
```

```
Intel 7115> list snmp_community
SNMP Community List
IP:  x.x.x.x => String : public =>
Rights : read
```

```
Intel 7115> delete snmp_community

SNMP Community String(s) Deletion.

<2> Current Available SNMP Community String(s):

1.) IP:         0.0.0.0 => String:    public

2.) IP:         0.0.0.0 => String:   private

Enter number (1 to 2) to delete (q to quit) [1]: 2

Enter number (1 to 2) to delete (q to quit) [1]: q
```

Trap Community String

Use CLI commands, **setsnmp trap_community**, **list trap_community** and **delete trap_community** to set, display, and delete trap community strings.

```
Intel 7115> setsnmp trap_community
SNMP Trap Community String(s) Setting.
Enter a SNMP Trap Community IP (q to quit): 0.0.0.0
Enter a SNMP Trap Community String (q to quit): private
Enter a SNMP Trap Community IP (q to quit): 0.0.0.0
Enter a SNMP Trap Community String (q to quit): public
Enter a SNMP Trap Community IP (q to quit): q


Intel 7115> list trap_community
SNMP Trap Community String(s) information.
<2> Current SNMP Trap Community String(s):
1.) IP:   0.0.0.0 => String: public
2.) IP:   0.0.0.0 => String:  private


Intel 7115> delete trap_community
SNMP Trap Community String(s) Deletion.
<2> Current Available SNMP Trap Community String(s):
1.) IP:   0.0.0.0 => String:   public
2.) IP:   0.0.0.0 => String:   private
Enter number (1 to 2) to delete (q to quit) [1]: 2
Enter number (1 to 2) to delete (q to quit) [1]: q
```

Access Control

The 7110/7115 provides **block** and **permit** commands which allow you to deny or allow clients to access servers based on IP, IP mask, port and port mask.

To block a client, specified by IP and IP mask, from accessing a specified server, use the **create block** command as illustrated below:

NOTE: To show, list or delete blocks and permits, see the Command Reference in Chapter 5.

```
Intel 7115> create block
Client IP to block [0.0.0.0]: 10.1.2.1
Client IP mask [0.0.0.0]: 255.255.255.255
Server IP to block [0.0.0.0]: 20.1.2.1
Server IP mask [0.0.0.0]: 255.255.255.255
Server Port to block: 80
Server Port mask [0xffff]:<Enter>
```

To permit a client, specified by IP and IP mask, access to a specified server, use the **create permit** command as illustrated below:

```
Intel 7115> create permit
Client IP [0.0.0.0]: 10.1.2.1
Client IP Mask [0.0.0.0]:255.255.255.255
Server IP [0.0.0.0]:20.1.2.1
Server IP Mask [0.0.0.0]:255.255.255.255
Server port [xx]: 443
Server port mask [0xffff]: <Enter>
```

Notes

7 Alarms and Monitoring

Overview

The Intel® NetStructure™ 7110/7115 e-Commerce Accelerator supports the configuration of alarms and to be sent to the console upon pre-designated events, and of periodic status-monitoring reports. Both alarms and monitor reports are single lines of text, with alarms being prefaced by the letter “A,” and monitor reports with the letter “M,”and both have timestamps. Both alarms and monitor reports can be written to the local administration console or to remote management sessions (Telnet or Secure Shell only).

Alarms can be configured to immediately notify the user of the following conditions:

- Encryption Status change
- Refused SSL connections
- Utilization (Threshold) alarms

- Overload alarms
- Network Link Status

All alarms are disabled by default and may be enabled in any combination.

Alarm format:

```
A:yyyymmddhhmmss:
ALARM_CODE:MODIFIER:EXTENDED_DATA:/
*message*/
```

Where:

`A:` Identifies the message as an alarm (as opposed to a monitor report).

`yyyymmddhhmmss:` The timestamp.

`ALARM_CODE:` The alarm type: `[ESC|RSC|UTL|OVL|NLS]`.

`MODIFIER:` The alarm modifier, a code identifying the event that triggered the alarm.

NOTE: *The Encryption Status Change alarm (ESC) does not display extended data.*

`EXTENDED_DATA:` Any additional relevant data.

`/*message*/:` Human-readable text description of the alarm.

The CLI commands for alarm configuration are:

Command	Parameters	Default
set alarms	all, esc, rsc, utl, ovl, nls	none
show alarms		

For example:

```
Intel 7115> set alarms
Select monitoring fields (all, esc, rsc,
utl, ovl, nls) [all]: all
Intel 7115> show alarms
All alarms are enabled.
Intel 7115> set alarms none
Intel 7115> show alarms
All alarms are disabled.
```

Alarm Types

The configurable alarm types are detailed in separate sections below.

ESC: Encryption Status Change Alarm

When enabled, an alarm is issued when the device is changed between INLINE and BYPASS modes. This change can be made from CLI using the commands, **inline** or **bypass**, or at the device's front panel by pressing the BYPASS button.

Format:

```
A:yyyymmddhhmmss:ESC:HDWR|CONB|CONI|FNTB|
FNTI|APPR:/*message*/
```

Where:

```
A: identifies the message as an alarm.
yyyymmddhhmmss: is the timestamp.
ESC: identifies the message as an Encryption
Status Change Alarm.
```

Alarm Modifiers and Messages:

```
HDWR: indicates crypto card failure
CONB: indicates console-controlled bypass
CONI: indicates console-controlled inline
```

```
FNTB: indicates front panel-controlled
bypass

FNTI: indicates front panel-controlled
inline

APPR: indicates application restart
```

RSC: Refused SSL Connections

When enabled, an alarm is generated whenever SSL connections are refused for cipher suite mismatch or client certificate authentication failure during the current user-specified period (5 to 65000 seconds, default: 15 seconds). The total number of refused SSL connections is reported along with the reason for refusal. This alarm can be enabled or disabled at the CLI.

Format:

```
A:yyyymmddhhmmss:RSC:CSMM|CCAF:XXX:
/*message*/
```

Where:

```
A: identifies the message as an alarm.

yyyymmddhhmmss: is the timestamp.

RSC: identifies the message as an Refused
SSL Connections Alarm.
```

Alarm Modifiers and Messages

```
CSMM: Cipher suite mismatch

CCAF: Client certificate authenticate
failure
```

Extended Data

```
XXX: An integer value indicating the number
of refused SSL connections that occurred in
the current alarm period.
```

RSC Alarm CLI Commands

To set Overload Alarm time window:

```
set rsc_window <seconds> (Range: 5-65000,
default: 15)
```

To display Overload Alarm time window

```
show rsc_window
```

Examples:

```
Intel 7115> set rsc_window 10
```

```
Intel 7115> show rsc_window
Check refused SSL connections [secs]: 10
```

UTL: Utilization Threshold Alarm

This alarm monitors three utilization threshold values:

- CPU
- Connections per Second
- Total Open Connections.

When enabled, an alarm is issued whenever any of the utilization values exceeds its high-water mark, or, having exceeded the high-water mark, drops below the low-water mark. The user defines the high and low-water marks. By default, the high-water mark is 90% and the low-water mark is 60%.

The data collected for utilization threshold metrics tends to be bursty, so a smoothing algorithm is used to prevent continuous alarms.The utilization window is a user-specified sliding interval during which data is collected and averaged. Consequently, shorter intervals are likely to result in some extraneous alarms. The interval can be set from 5 to 65000 seconds (default: 15).

Format:

```
A:yyyymmddhhmmss:UTL:ALRT|NMRL:CPU|CON|CPS:/
*message*/
```

Where:

```
A: identifies the message as an alarm.
```

```
yyyymmddhhmmss: is the timestamp.
```

```
UTL: identifies the message as an
Utilization Threshold Alarm.
```

Alarm Modifiers and Messages

```
ALRT: Message: [CPU|Open connections|CPS]
exceed high water mark
```

```
NMRL: Message: [CPU|Open connections|CPS]
drop below low water mark
```

Extended Data

```
CPU: Indicates that CPU Utilization
triggered the alarm.

CON: Indicates that Total Active Connections
triggered the alarm.

CPS: Indicates that Connections per Second
triggered the alarm.
```

UTL Alarm CLI commands

To set Utilization Threshold Alarm time window:

```
set utl_window <seconds> (Range: 5-65000,
default: 15)
```

To set Utilization Threshold Alarm high-water value:

```
set utl_high <percentage> (Range: 2-100,
default: 90)
```

To set Utilization Threshold Alarm low-water value:

```
set utl_low <percentage> (Range: 1-99,
default: 60)
```

To display current settings:

```
show utl_window

show utl_high

show utl_low
```

Examples:

```
Intel 7115> set utl_window 10

Intel 7115> show utl_window
Utilization window set [secs]: 10.

Intel 7115> set utl_highwater 80

Intel 7115> show utl_highwater

Utilization High water mark [%]: 80

Intel 7115> set utl_lowwater 60

Intel 7115> show utl_lowwater

Utilization Low water mark [%]: 60
```

OVL: Overload Alarm

WARNING: *This alarm indicates loss of encryption/decryption.*

When enabled, an alarm is issued upon occurence of overloads resulting in spills or throttles during the current user-configured alarm period (5 to 65000 seconds, default: 15 seconds).

Format:

```
A:yyyymmddhhmmss:OVL:SPIL|THRT:XXX:
/*message*/
```

Where:

`A: identifies the message as an alarm.`

`yyyymmddhhmmss: is the timestamp.`

`OVL: identifies the message as an Overload Alarm.`

Alarm Modifiers and Messages:

`SPIL: indicates overload resulting in a spill. Message: Spill mode.`

`THRT: indicates overload resulting in a throttle. Message: Throttle mode.`

Extended Data:

`XXX: An integer value indicating the total number of overload events that occurred during the most recent alarm period.`

OVL Alarm CLI Commands:

To set Overload Alarm time window:

`Intel 7115>` **`set ovl_window <seconds>`** `(Range: 5-65000, default: 15)`

To display Overload Alarm time window:

`Intel 7115> s`**`how ovl_window`**

Examples:

`Intel 7115>` **`set ovl_window 10`**

```
Intel 7115> show ovl_window
Check for overload conditions [sec]: 10
```

NLS: Network Link Status Alarm

An alarm is issued whenever the Network or Server link status is changed.

Format:

```
A:yyyymmddhhmmss:NLS:NETL|SVRL:LNKD|10HDX|10
FDX|100HDX|100FDX:/*message*/
```

Where:

A: identifies the message as an alarm.

yyyymmddhhmmss: is the timestamp.

NLS: identifies the message as a Network Link Status Alarm.

Alarm modifiers and messages:

NETL: indicates the network port status. Message: [No carrier|10Mb/s|100Mb/s][half duplex|full duplex]

SVRL indicates the server port status. Message: [No carrier|10Mb/s|100Mb/s] [half duplex|full duplex]

Extended Data:

LINKD: indicates no carrier.

10HDX: indicates 10Mb/s, half duplex.

10FDX: indicates 10Mb/s, full duplex.

100HDX: indicates 100Mb/s, half duplex.

100FDX: indicates 100Mb/s, full duplex.

Alarm Logging

The 7110/7115 maintains a circular buffer of alarms issued. The most recent alarms, as well as historical logs generated and saved as a result of exceptional conditions, are viewable at the console or in Telnet or Secure Shell (SSh) remote sessions. Viewing the current alarms results in an immediate dump of the alarm buffer.

The historical logs consist of a snapshot of the information retrievable via the **status line** command followed by a dump of the alarm buffer existing at the time of the exceptional condition.

These alarms can be viewed on the console using the CLI command, **status alarms**. Additionally, any logs generated and saved as a result of an exceptional condition are viewable by using the CLI command, **status <log filename>**. (A list of the viewable log files is displayed using the **list logs** command.)

Below are examples of the CLI commands for log viewing, the defaults, and ranges where applicable:

Examples, **list logs** and **status** commands:

```
Intel 7115> list logs

20000727_145544

Intel 7115> status 20000727_145544

================ STATE ====================

Boot time:                    Thu Jul 27 14:54:21
2000

Curr time:                    Thu Jul 27 14:55:43
2000

Restarts:                      3

KTR Mask:                      0xFFFFF3DD

Total Connections:             0

Active Connections:            0, 0 (cur, max)

Connections/Second:            0, 0 (cur, max)


Util Status:

Secure Bytes Read:             0

Plain Bytes Read:              0

Secure Bytes Wrote:            0

Plain Bytes Wrote:             0

Bytes Allocated to dbufs:      0

Bytes Per dbuf:                0


Spill Mode:                    disable
```

```
Transactions Spilled:           0
Times Thottled Accepts:         0
Bypass Mode:                    disable
L&M board status:               RESPEND  INLINE
(0x00000060)
Network NIC:                    100baseTX Half
Duplex
                                (0x00000026
0x00000003 0x00000026)
Server NIC:                     No carrier
                                (0x00000023
0x00000001 0x00000023)
Network LED:                    on
Server LED:                     off
Next heartbeat deadline:        never
SSL Caching:                    Enabled.

--------------- Configuration --------------
conlog 0xfffffef
ilog 0xffffffff
trace 0xfffff3dd
media auto
logport tty01
cache 3
server_tmo 5
client_tmo 30
serverif exp1
netif exp0
map 0.0.0.0 443 80 default
kpanic reboot
monitoring_interval 0
monitoring_fields 0x1f
alarm_mask 0x0000001f
```

```
ovl_window 15
rsc_window 15
utl_window 15
utl_high 90
utl_low 60
idle 300
kstrength 512
con_speed 9600
con_bits 8
con_stop 1
con_parity n
defcert_cname US
defcert_state California
defcert_city San Diego
defcert_orgname Intel Corporation
defcert_orgunit Network Equipment Division
defcert_name www.intel.com
defcert_email support@intel.com
prompt Intel 7115>
trap_authen
remote_if exp0
ip 10.1.11.34
netmask 255.255.0.0
A:07/27/2000 14:54:47:NLS:SVRL:NC:/* Server port
status, No carrier */
A:07/27/2000 14:54:41:NLS:SVRL:100FDX:/* Server
port status, 100Mb/s, full dupl/
A:07/27/2000 14:54:21:NLS:NETL:100HDX:/* Network
port status, 100Mb/s, half dup/
A:07/27/2000 14:54:21:NLS:SVRL:NC:/* Server port
status, No carrier */
A:01/01/1970 00:00:00:ESC:APPR:3:/* Application
Restarted */
Intel 7115>
```

Example, **status alarms** command:

```
Intel 7115> status alarms

A:07/27/2000 14:57:05:ESC:CONI:/* Console inline
*/

A:07/27/2000 14:57:05:NLS:NETL:100HDX:/* Network
port status, 100Mb/s, half dup/

A:07/27/2000 14:57:01:ESC:CONB:/* Console bypass
*/

A:07/27/2000 14:57:01:NLS:NETL:NC:/* Network port
status, No carrier */

A:07/27/2000 14:56:51:NLS:SVRL:NC:/* Server port
status, No carrier */

A:07/27/2000 14:56:46:NLS:SVRL:100FDX:/* Server
port status, 100Mb/s, full dupl/

A:07/27/2000 14:56:30:ESC:CONI:/* Console inline
*/

A:07/27/2000 14:56:30:NLS:NETL:100HDX:/* Network
port status, 100Mb/s, half dup/

A:07/27/2000 14:56:29:NLS:NETL:NC:/* Network port
status, No carrier */

A:07/27/2000 14:56:29:NLS:SVRL:NC:/* Server port
status, No carrier */

Intel 7115>
```

Monitoring

Monitoring Reports

A monitoring report is one line of user-configurable text displayed at the console at a user-configurable interval of between five and 65000 seconds. The interval default is 15 seconds.Console Configuration

Monitoring reports are disabled by default, and are enabled with the CLI **monitor...** command set. The monitoring application is aware of the port on which the enable command arrives, and accordingly sends reports to that same port, thus monitoring reports are displayed on the same console from which the feature is enabled.

Report Configuration

You can specify the fields to be displayed in each report. Reports begin with the letter “M” (for monitor report, to distinguish them from alarm reports) and the timestamp. The other fields available are user-selectable via a CLI command see “CLI Commands” this below in this section). The standard default fields are mode, failmode, CPU, SSLCS, and OVR. Monitor reports are disabled by default.

Monitor report format:

```
M:yyyymmddhhmmss:mode:failmode:CPU;i,k,a:SSL
CS;c,m,t:OVR;r,c,m,t:
NetIF;s:SvrIF;s:BES;c,m,t;BDS;c,m,t
```

Where:

```
M Monitor report

yyyymmddhhmmss Timestamp

mode Bypass mode status [INLINE|BYPASS]

failmode Fail mode status [SAFE|THRU]

CPU;i,k,a CPU%; (i)dle, (k)ernel,
(a)pplication

SSLCS;c,m,t SSL Connections per Second;
(c)urrent, (m)ax, (t)otal

OVR;r,c,m,t Overload events; (r)esponse
[SPIL|THRT], (c)urrent, (m)ax,
```

```
(t)otal

NetIF;s Net interface; (s)tatus
[NC|10HDX|10FDX|100HDX|100FDX]

SvrIF;s Svr interface; (s)tatus
[NC|10HDX|10FDX|100HDX|100FDX]

BES;c,m,t Bytes Encrypted per Second;
(c)urrent, (m)ax, (t)otal

BDS;c,m,t Bytes Decrypted per Second;
(c)urrent, (m)ax, (t)otal
```

Monitoring Reports CLI Commands

Below are the CLI commands for console monitoring, with defaults and ranges where applicable:

```
set monitoring_interval <seconds> (Range: 5-
65000; Default: 15 )

show monitoring_interval

set monitoring_fields <fields> (Range: all,
mode, failmode, cpu, cps, ovrld, link, enc,
dec; Default: mode, failmode, cpu, cps,
ovrld)

show monitoring_fields

set monitoring enable|disable (Default:
disable)

show monitoring
```

Examples:

```
Intel 7115> set monitoring_interval 15

Intel 7115> show monitoring_interval

Monitoring report interval [secs]: 15

Intel 7115> set monitoring disable

Intel 7115> show monitoring

The monitoring report is disabled for this
CLI.

Intel 7115> set monitoring_fields

Select monitoring fields (all, mode,
failmode, cpu, cps, ovrld, link, enc,

dec) [all]: all
```

```
Intel 7115> show monitoring_fields
All monitoring fields are enabled.
Intel 7115> set monitoring enable
Intel 7115> show monitoring
The monitoring report is enabled for this
CLI.
```

Notes

s

8 Software Updates

Use the **import upgrade** command to update/upgrade your Intel® NetStructure™ 7110/7115 e-Commerce Accelerator software. When you upgrade your 7110/7115 software, the configuration (including all keys, certificates, and mapping) is saved. However, all log files are cleared. The software is in the form of an image file (*.IMG).

Use the import patch command to install an Intel-provided patch to a current software release. Patches typically effect fixes to minor software issues. Intel Support can provide guidance regarding patches appropriate to your system, if any.

Using Windows§ HyperTerminal§

Command: **import upgrade**

Use the 7110/7115's aux console port, which defaults to 115.2 kbps, for greater speed. The import procedure (using xmodem) requires approximately 7 minutes at 115.2 kbps.

1. Download the image file (.IMG) to the local PC.
2. Connect the serial cable from COM1 or COM2 to the 7110/7115 auxiliary console.
3. Log in to the 7110/7115.
4. Type the **import upgrade** command. The command prompts for xmodem or uuencode. Press **Enter** to use the default (xmodem).

```
Intel 7115> import upgrade
Import protocol: (xmodem, uudecode)
[xmodem]: <Enter>
Start xmodem upload now
Use Ctl-X to cancel upload
```

5. In HyperTerminal§, click **Send File** from the Transfer menu, select the file (you can type the filename or click the **Browse** button to find the file), click to select the transfer protocol (1K xmodem), and click **Send**.

```
Verifying upgrade image...
Upgrade image valid
===  Release x.x
===  Load xx, Fri Aug 25 05:31:51 2000
```

WARNING: *All saved logs will be deleted and the system will reboot upon successful completion of the upgrade.*

6. Press **y** (for yes) at the "Continue with upgrade?" prompt.

```
Continue with upgrade? [n]: y
Upgrading...
System rebooting...done
```

Command: **import patch**

Use the 7110/7115’s aux console port, which defaults to 115.2 kbps, for greater speed. The import procedure (using xmodem) requires approximately 7 minutes at 115.2 kbps.

1. Download the patch file (.patch) to the local PC.
2. Connect the serial cable from COM1 or COM2 to the 7110/7115 auxiliary console.
3. Log in to the 7110/7115.
4. Type the **import patch** command. The command prompts for xmodem or uuencode. Press **Enter** to use the default (xmodem).

```
Intel 7115> import patch
Import protocol: (xmodem, uudecode)
[xmodem]: <Enter>
Start xmodem upload now
Use Ctl-X to cancel upload
```

5. In HyperTerminal§, click **Send File** from the Transfer menu, select the file (you can type the filename or click the **Browse** button to find the file), click to select the transfer protocol (1K xmodem), and click **Send**.

```
Verifying patch image...
Patch successfully imported.
```

The patch becomes effective upon the next system reboot. Should a patch fail upon import, the last successfully imported patch is reapplied.

Using Unix§ ‘cu’ and uuencoded image file

Command: **import upgrade**

1. Download the image file (assume the name is nn.img) to the local Unix§ machine.
2. Uuencode the image file.

```
uuencode nn.img nn.img >nn.uu
```

3. Connect the serial cable to the 7110/7115 auxiliary console.

4. Use the 'cu' program to connect to the 7110/7115 (Device name may vary depending on your operating system).

```
cu –l /dev/cuaa0 –s 115200
```

5. Log in to the 7110/7115.

6. Type the **import upgrade** command. At the prompt, press **u** or type **uudecode**.

```
Intel 7115>import upgrade

Import protocol: (xmodem, uudecode)
[xmodem]: u

Type or paste in data, end with ... alone on
line.
```

7. To send the uuencoded file use the "~>" command.

```
~>nn.uu

Verifying upgrade image...
Upgrade image valid
===  Release x.x
===  Load xx, Fri Aug 25 05:31:51 2000
```

WARNING: *All saved logs will be deleted and the system will reboot upon successful completion of the upgrade.*

8. Press **y** (for yes) at the "Continue with upgrade?" prompt.

```
Continue with upgrade? [n]: y
Upgrading...
System rebooting...done
```

Command: **import patch**

1. Download the patch file (assume the name is nn.patch) to the local Unix§ machine.

2. Uuencode the patch file.

```
uuencode nn.patch nn.patch >nn.uu
```

3. Connect the serial cable to the 7110/7115 auxiliary console.

4. Use the 'cu' program to connect to the 7110/7115 (Device name may vary depending on your operating system).

```
cu –l /dev/cuaa0 –s 115200
```

5. Log in to the 7110/7115.

6. Type the **import patch** command. At the prompt, press **u** or type **uudecode**.

```
Intel 7115>import patch

Import protocol: (xmodem, uudecode)
[xmodem]: u

Type or paste in data, end with ... alone on
line.
```

7. To send the uuencoded file use the “~>” command.

```
~>nn.uu

Verifying patch image...
Patch successfully imported.
```

Notes

9 Troubleshooting

Item	Symptom	Probable Cause	Remedy
1	Server and/or Network LEDs not illuminated.	• Unit is in Bypass mode. • Improper cabling.	• If the Inline LED is not illuminated (solid or blinking) take the 7110/ 7115 out of Bypass mode by either pressing the Bypass switch on the unit's front panel or using the CLI's **inline** command. • Depending on what type of equipment the 7110/7115 is connected to, either straight-through or crossover Cat-5 network cables are required for both Network and Server ports. Switch out the different cable types at each port until both Network and Server LEDs are illuminated.

Item	Symptom	Probable Cause	Remedy
2	Non-SSL data does not pass through 7110/7115.	Improper cabling.	• Refer to Item 1 in this table. • If both Network and Server LEDs are illuminated, configure the 7110/7115 to Fail-through mode (see Appendix B) and place the unit in Bypass mode. This effectively bypasses the 7110/7115, so if the problem persists its origin is elsewhere in the network.
3	Web pages are not completely displayed, or an error message such as, "Document Contains No Data" appears.	The client timeout value is too small. "Client timeout" is the interval that the connection between the client and server can remain idle (i.e., no data crosses the connection in either direction) following a client request.	Increase the interval with the following command: `Intel 7115> set client_tmo <n>` where <n> is the interval in seconds. The default is five seconds. The recommended value is 1.5 times the longest server response time.
4	SSL traffic does not pass through 7110/7115	• Improper mappings. • Improper cabling.	• See *Mapping* in Chapter 3. • See Item 1 in this table.
5	Error message: The page cannot be displayed.	The digital certificate and/or private key is corrupt.	Use the default key and certificate, or create new key and unsigned certificate. Try the page again. If the error no longer appears, recreate your private key and certificate signing request (CSR) and resubmit to the certificate authority to get a new certificate.

Item	Symptom	Probable Cause	Remedy
6	Error message indicates that the browser does not recognize the signer of this certificate after loading global server ID.	The intermediate certificate is not installed or is installed improperly.	See *Global Site Certificates* in Chapter 3 for correct procedures.

Item	Symptom	Probable Cause	Remedy
7	Error message: Server/Network media mismatch	Server and network ports have autonegotiated to different media settings.	Use the **status** command to determine the media settings: `Intel 7115> status` `.` `.` `Network port 100baseTX Full Duplex` `Server port  10baseT, Half Duplex` Then use the **nic** command to force common media attributes, e.g.: `Intel 7115> nic` `1 - auto` `2 - 10baseT, half duplex` `3 - 10baseT, full duplex` `4 - 100baseTX, half duplex` `5 - 100baseTX, full duplex` `Select media type [1] 2` In the example above, 2 is the correct choice because the setting must reflect the “least common denominator” of both media speed and duplex attribute, i.e., the server port is determinative because it has both the lower speed and lower (half) duplex attribute.

A Front Panel

The following diagram shows the LEDs, buttons, switches and connections for the Intel® NetStructure™ 7110/7115 e-Commerce Accelerator. Note that there is no power switch or button. Power is applied to the device by connecting the power cable.

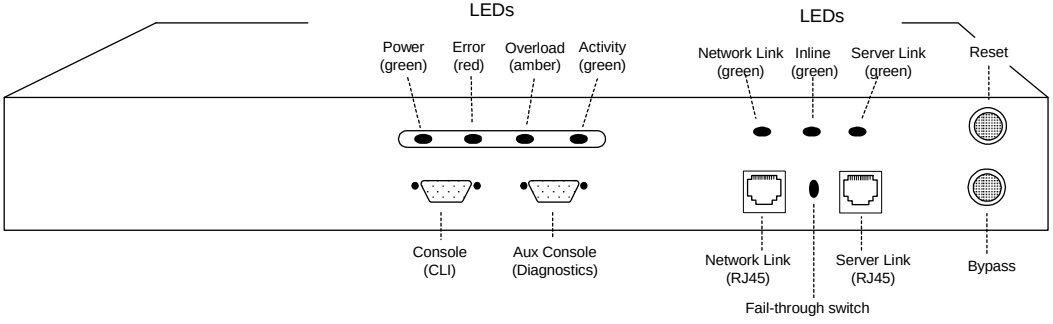

Figure A-1: Front Panel Connectors, Controls, and Indicators

Buttons and Switches

There are two buttons and one switch on the front panel of the 7110/7115.

Button/Switch	Action
Reset button	Press momentarily to issue a soft reset to the 7110/7115. Press for 5 seconds to reset the 7110/7115 and restore the factory defaults.
Bypass button	Press to physically force bypass mode (bypass 7110/7115 processing).
Fail-through/ Fail-safe switch	**Default**: Fail-safe (up position), the network connection is broken during a 7110/7115 failure. Fail-through (down position), the network connection is maintained during a 7110/7115 failure. Refer to *Failure/Bypass Modes* in Appendix B for details.

Front Panel LEDs

The LED display provides high-level 7110/7115 information. There are seven LEDs on the 7110/7115's front panel, in two groups of four and three, respectively.

LED	Status
Power	ON – Power is supplied to 7110/7115.
	OFF – No Power to 7110/7115.
Error	ON – Error condition found.
	OFF – Normal operation.

LED	Status
Overload	ON – 7110/7115 is saturated with SSL requests. LED ranges from dim flickering to bright steady, indicating low to high spillover. Refer to the spill command for ways to offload requests to another 7110/7115.
	OFF – Normal operation.
Activity	ON – SSL processing is being performed. Ranges from dim, when processing loads are low to bright, when greater amounts of processing are occuring.
	OFF – No SSL processing is being performed.
Network Link	ON – Operational network connection.
	OFF – No operational network connection.
Inline (See Appendix B, *Failure/ Bypass Modes*)	BLINKING GREEN – Fail-safe mode, which is the default. In the event of a 7110/7115 failure, traffic will not pass through.
	STEADY GREEN – Fail-through mode, which allows traffic to pass even with 7110/7115 failure.
	OFF – 7110/7115 is not operational, or is in Bypass mode.
Server Link	ON – Operational server connection.
	OFF – No operational server connection.

Connectors

The following table describes the 7110/7115's connectors.

Designator	Type	Purpose
Network	RJ45	100baseTX/10baseT connection to network (clients), wired as a host port.
Server	RJ45	100baseTX/10baseT connection to server (or servers), wired as a hub port.
Console	DB9	RS-232 DTE console port (9600 8, N, 1)
Aux Console	DB9	RS-232 DTE console port (115200, 8, N, 1) includes kernel diagnostics at boot.
Power		Power input

B Failure/Bypass Modes

WARNING: *Enabling bypass mode will instantly and without warning terminate all active remote management sessions.*

The Intel® NetStructure™ 7110/7115 e-Commerce Accelerator is designed with the ability to automatically bypass e-Commerce traffic in the event of a failure. If necessary, the user can force a bypass with the Bypass button or from the command line interface using the bypass command. There is also a security feature (Fail-through switch). In the default Fail-safeFail-safe position, this switch prevents traffic from passing through unprocessed in the event of a failure or if Bypass mode is manually activated.

The following discussion about the Bypass button and Fail-through switch assumes that normal conditions for 7110/7115 processing are in effect (i.e., the user has entered the appropriate CLI commands to enable 7110/7115 processing).

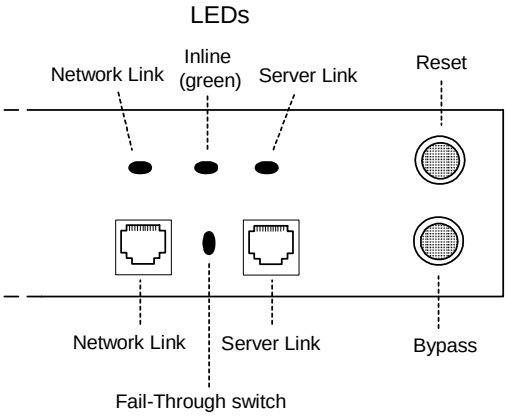

Figure B-1: Front Panel Detail: Failure/Bypass Mode Controls and Indicators

Bypass Button

Forcing a bypass of the 7110/7115 may be necessary when certain actions must be performed offline (e.g., configuration changes, entering certificates, or problem isolation).

To force a bypass of 7110/7115 processing, push the Bypass button ON. The Network Link, Inline, and Server Link LEDs are off in Bypass mode. ON disables the 7110/7115's ability to process e-Commerce traffic. The mode of the Fail-through switch controls whether traffic continues to flow unprocessed between the client and the server (discussed below).

Fail-through Switch (Security Level)

This switch allows the user to control what happens in the event of a failure. It is located in a recess between the network link and server link connectors. Use a small screwdriver or paper clip to manipulate the switch. The two options are to either let traffic flow through the 7110/7115 in the event of a failure (or the Bypass Switch being on)

or to be blocked. When the switch is in Fail-through mode (down position), traffic is allowed to pass through unprocessed in the event of a failure of the 7110/7115 or if the Bypass toggle is ON.

During normal processing, the Inline (green) LED on the front panel indicates whether e-Commerce traffic will pass through in the event of a failure (depending on Fail-through switch state). Steady green or blinking green both mean that the 7110/7115 is processing traffic; blinking green indicates traffic will be blocked if the 7110/7115 fails (Fail-safe mode), and steady green indicates traffic will continue (unprocessed) in the event of a failure (Fail-through mode). When the Inline LED is off, no SSL processing is taking place, which means either no traffic is passing through (Fail-safe), or the traffic that is passing through is unprocessed (Fail-through).

The following conditions and Inline LED behavior are possible with the Fail-through switch and Bypass button:

Device Mode	Bypass Button	Fail-through Switch Mode	Traffic Status	Inline LED
Failed	N/A	Fail-safe (Up position)	No traffic (either direction)	off
Failed	N/A	Fail-through (Down position)	Passes through unprocessed	off
N/A	ON (Bypass)	Fail-safe (Up position)	No traffic (either direction)	off
N/A	ON (Bypass)	Fail-through (Down position)	Passes through unprocessed	off
Operational	OFF (Inline)	Fail-safe (Up position)	Processing	Blinking green
Operational	OFF (Inline)	Fail-through (Down position)	Processing	Steady green

Notes

C Supported Ciphers

The Intel® NetStructure™ 7110/7115 e-Commerce Accelerator supports only RSA key exchange and authentication. Diffie-Hellman (including Anonymous and Ephemeral) key exchange/authentication and DSS authentication are not supported.

Use the **set cipher** command to specify the cipher. The command prompts you for the cipher strength and SSL version level. Options for these values are:

Cipher Strength

- **All** - all supported ciphers (including export ciphers)
- **High** - all ciphers with 168-bit encryption (Triple-DES)
- **Medium** - all ciphers with 128-bit and higher encryption (including High)
- **Low** - all ciphers with 64-bit and higher encryption (including Medium and High)
- **Export only** - all export ciphers

SSL Version Level

- **SSLv2** - all SSL version 2.0 ciphers
- **SSLv3** - all SSL version 3.0 ciphers
- **SSLv2** and **SSLv3** - all SSL version 2.0 and 3.0 ciphers

The default cipher value is **all supported ciphers** (both SSLv2 and SSLv3).

The following table provides ciphers supported by the 7110/7115. Note that the export version of the software supports only the ciphers marked “E” in the Profile column.

Name	Protocol	Key Exchange	Authentication	Encryption (key size)	Message Authentication	Profile (Hi/ Medium/ Low/ Export)
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES(168)	SHA1	H
IDEA-CBC-SHA	SSLv3	RSA	RSA	IDEA(128)	SHA1	M
RC4-SHA	SSLv3	RSA	RSA	RC4(128)	SHA1	M
RC4-MD5	SSLv3	RSA	RSA	RC4(128)	MD5	M
DES-CBC-SHA	SSLv3	RSA	RSA	DES(56)	SHA1	L
DES-CBC3-MD5	SSLv2	RSA	RSA	3DES(168)	MD5	H
IDEA-CBC-MD5	SSLv2	RSA	RSA	IDEA(128)	MD5	M

Name	Protocol	Key Exchange	Authentication	Encryption (key size)	Message Authentication	Profile (Hi/ Medium/ Low/ Export)
RC2-CBC-MD5	SSLv2	RSA	RSA	RC2(128)	MD5	M
RC4-MD5	SSLv2	RSA	RSA	RC4(128	MD5	M
RC4-64-MD5	SSLv2	RSA	RSA	RC4(64)	MD5	L
DES-CBC-MD5	SSLv2	RSA	RSA	DES(56)	MD5	L
EXP-DES-CBC-SHA	SSLv3	RSA(512)	RSA	DES(40)	SHA1	E
EXP-RC2-CBC-MD5	SSLv3	RSA(512)	RSA	RC2(40)	MD5	E
EXP-RC4-MD5	SSLv3	RSA(512)	RSA	RC4(40)	MD5	E
EXP-RC2-CBC-MD5	SSLv2	RSA(512)	RSA	RC2(40)	MD5	E
EXP-RC4-MD5	SSLv2	RSA(512)	RSA	RC4(40)	MD5	E

Notes

D Regulatory Information

Taiwan Class A EMI Statement

警告使用者 ：
這是甲類的資訊產品， 在居住的環境中使用時，
可能會造成射頻干擾， 在這種情況下，使用者會
被要求採取某些適當的對策。

VCCI Statement

Class A ITE

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Internal access to Intel® Express switches is intended only for qualified service personnel.

FCC Part 15 Compliance Statement

This product has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This product generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning this equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Change the direction of the radio or TV antenna.
- To the extent possible, relocate the radio, TV, or other receiver away from the product.
- Plug the product into a different electrical outlet so that the product and the receiver are on different branch circuits.

If these suggestions don't help, consult your dealer or an experienced radio/TV repair technician for more suggestions.

NOTE: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CAUTION: If you make any modification to the equipment not expressly approved by Intel, you could void your authority to operate the equipment.

Canada Compliance Statement (Industry Canada)

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques", NMB-003 édictée par le Ministre Canadien des Communications.

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled: "Digital Apparatus," ICES-003 of the Canadian Department of Communications.

CE Compliance Statement

This Intel® NetStructure™ 7110 e-Commerce Accelerator complies with the EU Directive, 89/336/EEC, using the EMC standards EN55022 (Class A) and EN55024:1998. This product also complies with the EU Directive, 73/23/EEC, using the safety standard EN60950.

CISPR 22 Statement

WARNING: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

VCCI Class A (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Australia

WARNING

The system is designed to operate in a typical office environment. Choose a site that is:

- Clean and free of airborne particles (other than normal room dust).
- Well-ventilated and away from sources of heat including direct sunlight.
- Away from sources of vibration or physical shock.

- Isolated from strong electromagnetic fields produced by electrical devices.
- In regions that are susceptible to electrical storms, we recommend you plug your system into a surge suppressor and disconnect telecommunication lines to your modem during an electrical storm.
- Provided with a properly grounded wall outlet.

Do not attempt to modify or use the supplied AC power cord if it is not the exact type required.

Ensure that the system is disconnected from its power source and from all telecommunications links, networks, or modem lines whenever the chassis cover is to be removed. Do not operate the system with the cover removed.

AVERTISSEMENT

Le système a été conçu pour fonctionner dans un cadre de travail normal. L'emplacement choisi doit être:

- Propre et dépourvu de poussière en suspension (sauf la poussière normale).
- Bien aéré et loin des sources de chaleur, y compris du soleil direct.
- A l'abri des chocs et des sources de ibrations.
- Isolé de forts champs magnétiques géenérés par des appareils électriques.
- Dans les régions sujettes aux orages magnétiques il est recomandé de brancher votre système à un supresseur de surtension, et de débrancher toutes les lignes de télécommunications de votre modem durant un orage.
- Muni d'une prise murale correctement mise à la terre.

Ne pas utiliser ni modifier le câble d'alimentation C. A. fourni, s'il ne correspond pas exactement au type requis.

Assurez vous que le système soit débranché de son alimentation ainsi que de toutes les liaisons de télécomunication, des réseaux, et des lignes de modem avant d'enlever le capot. Ne pas utiliser le système quand le capot est enlevé.

WARNUNG

Das System wurde für den Betrieb in einer normalen Büroumgebung entwickelt. Der entwickelt. Der Standort sollte:

- sauber und staubfrei sein (Hausstaub ausgenommen);
- gut gelüftet und keinen Heizquellen ausgesetzt sein (einschließlich direkter Sonneneinstrahlung);
- keinen Erschütterungen ausgesetzt sein;
- keine starken, von elektrischen Geräten erzeugten elektromagnetischen Felder aufweisen;
- in Regionen, in denen elektrische Stürme auftreten, mit einem Überspannungsschutzgerät verbunden sein; während eines elektrischen Sturms sollte keine Verbindung der Telekommunikationsleitungen mit dem Modem bestehen;
- mit einer geerdeten Wechselstromsteckdose ausgerüstet sein.

Versuchen Sie nicht, das mitgelieferte Netzkabel zu ändern oder zu verwenden, wenn es sich nicht um genau den erforderlichen Typ handelt.

Das System darf weder an eine Stromquelle angeschlossen sein noch eine Verbindung mit einer Telekommunikationseinrichtung, einem Netzwerk oder einer Modem-Leitung haben, wenn die Gehäuseabdeckung entfernt wird. Nehmen Sie das System nicht ohne die Abdeckung in Betrieb.

AVVERTENZA

Il sistema è progettato per funzionare in un ambiente di lavoro tipico. Scegliere una postazione che sia:

- Pulita e libera da particelle in sospensione (a parte la normale polvere presente nell'ambiente).
- Ben ventilata e lontana da fonti di calore, compresa la luce solare diretta.
- Al riparo da urti e lontana da fonti divibrazione.
- Isolata dai forti campi magnetici prodotti da dispositivi elettrici.

- In aree soggette a temporali, è consigliabile collegare il sistema ad un limitatore di corrente. In caso di temporali, scollegare le linee di comunicazione dal modem.
- Dotata di una presa a muro correttamente installata.

Non modificare o utilizzare il cavo di alimentazione in c. a. fornito dal produttore, se non corrisponde esattamente al tipo richiesto.

Prima di rimuovere il coperchio del telaio, assicurarsi che il sistema sia scollegato dall'alimentazione, da tutti i collegamenti di comunicazione, reti o linee di modem. Non avviare il sistema senza aver prima messo a posto il coperchio.

ADVERTENCIAS

El sistema está diseñado para funcionar en un entorno de trabajo normal. Escoja un lugar:

- Limpio y libre de partículas en suspensión (salvo el polvo normal)
- Bien ventilado y alejado de fuentes de calor, incluida la luz solar directa.
- Alejado de fuentes de vibración.
- Aislado de campos electromagnéticos fuertes producidos por dispositivos eléctricos.
- En regiones con frecuentes tormentas eléctricas, se recomienda conectar su sistema a un eliminador de sobrevoltage y desconectar el módem de las líneas de telecomunicación durante las tormentas.
- Previsto de una toma de tierra correctamente instalada.

No intente modificar ni usar el cable de alimentación de corriente alterna, si no se corresponde exactamente con el tipo requerido.

Asegúrese de que cada vez que se quite la cubierta del chasis, el sistema haya sido desconectado de la red de alimentación y de todos lo enlaces de telecomunicaciones, de red y de líneas de módem. No ponga en funcionamiento el sistema mientras la cubierta esté quitada

Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät is vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.

15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einerqualifizierten Servicestelle zu überprüfen:
    a. Netzkabel oder Netzstecker sint beschädigt.
    b. Flüssigkeit ist in das Gerät eingedrungen.
    c. Das Gerät war Feuchtigkeit ausgesetzt.
    d. Wenn das Gerät nicht der Bedienungsanleitung ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
    e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
    f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
16. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanscluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

Notes

E Terms and Conditions and Software License

Intel Corporation

END USER TERMS AND CONDITIONS OF SALE AND SOFTWARE LICENSE

IF THE PRODUCT IS PURCHASED DIRECTLY FROM INTEL AND UNLESS SUCH PARTIES HAVE ENTERED INTO A BILATERALLY EXECUTED AGREEMENT, WHICH EXPRESSLY TAKES PRECEDENCE, THE TERMS AND CONDITIONS STATED HEREIN WILL APPLY.

IF THE PRODUCT WAS PURCHASED FROM AN INTEL CHANNEL PARTNER, THEN ONLY SECTIONS 13-23 APPLY TO THE END USER.

1. **Entire Agreement:** These terms and conditions ("Agreement") for the sale of hardware and license of software, which includes the associated documentation shipped with the hardware and software ("Product"), constitute the complete and exclusive statement of all the terms of the Agreement between Intel Corporation, ("Intel") and the purchaser using the Product for its ordinary internal operation of its business and not for resale ("End User") and supersedes all prior understandings, writings, proposals, representations or communications, oral or written, relating to the subject matter hereof and unless subsequent different, contradictory or additional terms and conditions are agreed to in a writing signed by authorized representatives of both parties. In no event shall this Agreement be deemed an acceptance by Intel of any terms and conditions included with End User's purchase order or similar End User document.

Intel's performance hereunder is expressly conditioned on End User's assent to this Agreement.

2. **Orders:** End User may purchase Product by submitting a valid purchase order ("Order") to Intel at the corporate address stated herein. Orders are subject to Intel's written acceptance ("Order Acceptance"). Order Acceptance is based in part to approval of credit by Intel to End User as set forth in the "Credit Terms" Section of this Agreement.
3. **Term and Termination Date:** This Agreement shall be effective on the date of the Order Acceptance and continue in effect until terminated by either party upon thirty (30) days advance written notice unless terminated earlier for breach.
4. **Price:** The price to be paid by End User shall be that stated on the Order as accepted on the Order Acceptance. All prices are in U.S. dollars.
5. **Credit Terms:** Credit terms are made at Intel's sole discretion by analysis of End User's current and historical financial and credit information, bank and trade references, payment practices, etc. End User agrees to provide such information to Intel upon request. Intel reserves the right to refuse payment terms if, in Intel's sole discretion, such terms would create an unreasonable credit risk. In that event, deliveries will be available only on a C.O.D., cash-in-advance, or irrevocable letter of credit basis.
6. **Delivery:** Subject to the Section below entitled "Leasing/Renting," if applicable, Products shall be shipped Ex Works (1990 Incoterms), Intel's shipping dock. End User is responsible for payment of all costs relating to transportation, delivery, and insurance, which shall be pre-paid by Intel and added to the invoice, unless otherwise agreed to on the Order Acceptance. Title and risk of loss shall pass to End User upon delivery to the first common carrier except that shipments to destinations outside of the United States are subject to the "Security Interest and Reservation of Title" Section of this Agreement.
7. **Security Interest And Reservation Of Title:** End User hereby grants to Intel a purchase money security interest covering each shipment of Products made hereunder (and any proceeds thereof) in the amount of Intel's invoice for such shipment until Intel receives payment in full. (A purchase money security interest only applies to Products purchased by End User and the proceeds from the sale of such Products by End User.) End User agrees to sign and execute any and all documents as required by Intel to perfect such security interest. For Products shipped to destinations outside of the United States, Intel reserves title in such Products until End User pays Intel in full for such Products, at which time title in such Products shall pass to End User (except that in the case of software, only title to the media shall pass).
8. **Cancellation:** Orders cancelled within five (5) days of scheduled shipment may be subject to a ten percent (10%) cancellation charge.
9. **Payment Terms:** Payment in full is due thirty (30) days after date of the invoice. Intel may charge End User interest on any delinquent balance

at the lesser of eighteen percent (18%) per year or the maximum amount permitted by law. Intel may refuse shipment to End User if End User is delinquent in making payments to Intel.

10. **Taxes and Duties:** End User is responsible for all taxes imposed in connection with sale to End User of Products or services which Intel may incur under this Agreement (except taxes imposed on Intel's income) including but not limited to all import duties, customs fees, levies or imposts, and all sales, use, value added, gross receipts or other taxes of any nature and any penalties, interest and collection or withholding costs associated with any of the foregoing items. All such amounts are in addition to other amounts payable hereunder and this obligation shall survive termination or expiration of this Agreement. If applicable law requires End User to withhold any income taxes levied by the authorities of Canada on payments to be made pursuant to this Agreement ("Withholding Tax"), End User shall take advantage of the reduced Withholding Tax provided for by the Canada-United States tax treaty then in force and shall be entitled to deduct such Withholding Tax from the payments due to Intel hereunder. End User is further responsible for obtaining import licenses and preparing and submitting all required documentation in connection with importing Products including obtaining and providing to Intel International Import Certificates and other supporting documentation required by Intel in order to apply for United States export licenses.

11. **Leasing/Renting:** Subject to the provisions of this Section, End User may request to have Products delivered to it under a leasing/renting arrangement between End User and a lessor/owner ("Lessor"). Intel's obligations to accept any Order from Lessor and to deliver Product pursuant to such Order from Lessor are limited to the following circumstances:

    11. 1. The Lessor is Intel who will retain title to the Product and accept lease or rent payments; or

    11. 2. Any Lessor, other than Intel Order, provided that:

        11. 2. 1. The Order indicates on its face that Lessor is ordering the Product identified in the Order on behalf of End User;

        ii. The Order indicates on its face that it is in accordance with, and subject to,

        iii. The terms and conditions of this Agreement; and

        iv. Intel's credit department has approved the Lessor.

    With respect to any Order issued by any Lessor, other than Intel, subject to any specific provisions found in a bilaterally-executed agreement between Intel and Lessor, Lessor will be considered End User's agent for the purpose of ordering Product and making payment and the rights and obligations of End User and Intel identified in this Agreement shall remain except for the following:

        (1). Title to Product delivered pursuant to such Order shall be presumed vested in Lessor;

(2). The license accompanying the Product shall apply to Lessor; and

(3). Notwithstanding anything to the contrary in the license accompanying the Product, Lessor may transfer such title and license rights to End User under a leasing arrangement.

12. **Returns:** No Product may be returned except under warranty for repair or due to shipment error by Intel.

---

13. **Software License:** Intel grants End User a non-exclusive, non-transferable (except as set forth in this Section) non-exclusive, restricted right to use the Intel® software as incorporated in or supplied with the Intel hardware and solely in connection with the operation of the Product for End User's own internal business purposes. End User understands that Intel may update the Intel Product from time to time and such changes shall be subject to this license grant. End User may transfer the license to use the Intel software only in connection with a sale or transfer of the Product and as included with the Product and not on a standalone basis, provided the transferee agrees to be bound by the terms and condition of this Agreement. Intel and its suppliers retain all title to, and, except as expressly licensed herein, all rights to the software, all copies thereof, and all related documentation and materials. End User may not use, copy, modify, create derivative works of, distribute, sell, assign, pledge, sublicense, lease, loan, rent, timeshare, deliver or otherwise transfer the Intel software, nor permit any other party to do any of the foregoing.

14. **No Modifications To Product:** Product is shipped in its complete form and structure; no modifications are needed. End User shall not, nor permit any other party to modify, reverse engineer, reverse compile, or disassemble any part of Product, including any attempt to translate the Intel software, derive or attempt to derive the software source code or any part thereof. Any modification or attempt described herein will void the warranties of this Agreement.

15. **Limited Software Warranty:** Intel warrants to the first End User purchaser that the media containing the software is free from defects for a period of ninety (90) days from date of shipment. End User assumes responsibility for the selection of the appropriate network or computing equipment, software, and associated materials. Intel makes no warranty or representation that the software will work in combination with any third-party network or computing equipment or software, that the operation of the software will be uninterrupted or error free, or that all defects in the software will be corrected. No updates are provided under this Agreement. No warranties for third party software are provided by this warranty.

16. **Limited Hardware Warranty:** Intel warrants to the original owner that the product delivered in this package will be free from material defects in material and workmanship for one (1) year following the latter of: (i) the date of purchase only if you register by returning the registration card as indicted thereon with proof of purchase; or (ii) the date of manufacture; or (iii) the registration date if by electronic means provided such registration occurs within 30 days from purchase. This warranty does not cover the product if it is damaged in the process of being installed.

THE ABOVE WARRANTY IS IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT, OR ANY WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

This warranty does not cover replacement of products damaged by abuse, accident, misuse, neglect, alteration, repair, disaster, improper installation or improper testing. If the product is found to be otherwise defective, Intel, at its option, will replace or repair the product at no charge except as set forth below, provided that you deliver the product along with a return material authorization (RMA) number (see below) either to the company from whom you purchased it or to Intel. If you ship the product, you must assume the risk of damage or loss in transit. You must use the original container (or the equivalent) and pay the shipping charge. Intel may replace or repair the product with either a new or reconditioned product, and the returned product becomes Intel's property. Intel warrants the repaired or replaced product to be free from defects in material and workmanship for a period of the greater of: (i) ninety (90) days from the return shipping date; or (ii) the period of time remaining on the original one (1) year warranty.

This warranty gives you specific legal rights and you may have other rights which vary from state to state. All parts or components contained in this product are covered by Intel's limited warranty for this product; the product may contain fully tested, recycled parts, warranted as if new. For warranty information call one of the numbers below.

Returning a Defective Product (RMA): Before returning any product, contact an Intel Customer Support Group and obtain an RMA number by calling the non-toll free numbers below:

North America only: (800) 838-7136 or (916) 377-7000
Other locations: Return the product to the place of purchase.

If the Customer Support Group verifies that the product is defective, they will have the Return Material Authorization Department issue you an RMA number to place on the outer package of the product. Intel cannot accept any product without an RMA number on the package.

Limitation of Liability and Remedies: INTEL SHALL HAVE NO LIABLILITY FOR ANY INDIRECT OR SPECULATIVE DAMAGES (INCLUDING, WITHOUT LIMITING THE FOREGOING, CONSEQUENTIAL, INCIDENTAL AND SPECIAL DAMAGES) ARISING FROM THE USE OF OR INABILITY TO USE THE PRODUCT, WHETHER ARISING OUT OF CONTRACT, NEGLIGENCE, TORT, OR UNDER ANY WARRANTY, IRRESPECTIVE OF WHETHER INTEL HAS ADVANCED NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES, INCLUDING, BUT NOT LIMITED TO LOSS OF USE, INFRINGEMENT OF INTELLECTUAL PROPERTY, BUSINESS INTERRUPTIONS, AND LOSS OF PROFITS, NOTWITHSTANDING THE FOREGOING, INTEL'S TOTAL LIABILITY FOR ALL CLAIMS UNDER THIS AGREEMENT SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THESE LIMITATIONS ON POTENTIAL LIABILITES WERE AN ESSENTIAL ELEMENT IN SETTING THE PRODUCT PRICE. INTEL NEITHER ASSUMES NOR AUTHORIZES ANYONE TO ASSUME FOR IT ANY OTHER LIABILITIES.

Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions may not apply to you.

Europe only

Intel warrants to the original owner that the product delivered in this package will be free from defects in material and workmanship for one (1) year following the later of: (i) the date of purchase only if you register by returning the registration card as indicated thereon with proof of purchase; or (ii) the date of manufacture; or (iii) the registration date if by electronic means provided such registration occurs within 30 days from purchase. This warranty does not cover the product if it is damaged in

the process of being installed.

THE ABOVE WARRANTY IS IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT, OR ANY WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

This warranty does not cover replacement of products damaged by abuse, accident, misuse, neglect, alteration, repair, disaster, improper installation or improper testing. If the product is found to be otherwise defective, Intel, at its option, will replace or repair the product at no charge except as set forth below, provided that you deliver the product along with a return material authorization (RMA) number (see below) either to the company from whom you purchased it or to Intel. If you ship the product, you must assume the risk of damage or loss in transit. You must use the original container (or the equivalent) and pay the shipping charge. Intel may replace or repair the product with either a new or reconditioned product, and the returned product becomes Intel's property. Intel warrants the repaired or replaced product to be free from defects in material and workmanship for a period of the greater of: (i) ninety (90) days from the return shipping date; or (ii) the period of time remaining on the original one (1) year warranty.

All parts or components contained in this product are covered by Intel's limited warranty for this product; the product may contain fully tested, recycled parts, warranted as if new. For warranty information call one of the numbers below.

English	+44 1793 404900
French	+44 1793 404988
German	+44 1793 404777
Italian	+44 1793 404141

Returning a Defective Product (RMA): Return the product to the place of purchase for a refund or replacement.

Limitation of Liablility and Remedies: INTEL SHALL HAVE NO LIABILITY FOR ANY INDIRECT OR SPECULATIVE DAMAGES (INCLUDING, WITHOUT LIMITING THE FOREGOING, CONSEQUENTIAL, INCIDENTAL AND SPECIAL DAMAGES) ARISING FROM THE USE OF OR INABILITY TO USE THIS PRODUCT, WHETHER ARISING OUT OF CONTRACT, NEGLIGENCE, TORT, OR UNDER ANY WARRANTY, IRRESPECTIVE OF WHETHER INTEL HAS ADVANCE NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES, INCLUDING BUT NOT LIMITED TO LOSS OF USE, BUSINESS INTERRUPTIONS, AND LOSS OF PROFITS, NOTWITHSTANDING THE FOREGOING, INTEL'S TOTAL LIABILITY FOR ALL CLAIMS UNDER THIS AGREEMENT SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THESE LIMITATIONS ON POTENTIAL LIABILITIES WERE AN ESSENTIAL ELEMENT IN SETTING THE PRODUCT PRICE. INTEL NEITHER ASSUMES NOR AUTHORIZES ANYONE TO ASSUME FOR IT ANY OTHER LIABILITIES.

This limited Hardware Warranty shall be governed by and construed in accordance with the Laws of England and Wales. The courts of England shall have exclusive jurisdiction regarding any claim brought under this warranty.

17. **Export Law Regulations:**

17. 1. Applicable Laws. End User acknowledges that all Products, spares, documentation or other materials (collectively "Product") are subject to applicable import and export regulations of the United States and of the countries in which End User transacts business, specifically including U.S. Export Administration Act and Export Administration Regulations. This Agreement is also specifically subject to U.S. Department of Commerce regulations relating to restrictive trade practices or boycotts and the Foreign Corrupt Practices Act. In no event shall Intel be bound by any terms and conditions which contravene applicable laws. End User shall comply with all laws and regulations applicable to the Product. Without limiting the generality of the foregoing, End User agrees that it shall not export, re-export, transfer or divert any of the Product or the direct product thereof to any restricted place or party in accordance with U.S. export regulations.

17. 2. License Exceptions. End User acknowledges that certain of the Product are exported under U.S. Export Administration Regulation license exceptions which prohibit transfer, export or re-export to military end-users or for military uses or for use with regard to nuclear, chemical or biological weapons activity including projects, design, production or stockpiling such weapons. End User is responsible for compliance with all such license exceptions.

17. 3. Responsibility for Export Licensing. Intel agrees to use commercially reasonable steps to obtain, at Intel's expense, all documentation required by the United States Office of Export Administration and/or other authorities to permit the exportation of Product to End User. End User shall take all actions and provide all information reasonably requested by Intel in order for Intel to obtain such export licenses. Intel shall have no liability or obligation to End User if the responsible government authorities decline to issue any such export licenses. ALL ORDERS ISSUED PURSUANT TO THIS AGREEMENT ARE SUBJECT TO THE OBTAINING SAID LICENSES.

17. 4. Import Certificates. End User is responsible for obtaining and providing to Intel International Import Certificates and other supporting documentation required by Intel in order to apply for United States export licenses.

17. 5. Encrypted Products. Products containing encryption may require additional restrictions. Sale of these specific items may require End User's written consent to comply with any such additional restrictions prior to shipment of the Products.

17. 6. Letter of Compliance. Intel may require End User to execute a Letter of Compliance, as it deems reasonable to meet the requirements of applicable export regulations.

18. **United States Government Legend:** The software and documentation is commercial in nature and developed solely at private expense. The software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in this Agreement. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov. 1995) or FAR 52.227-14 (June 1987), whichever is applicable.

19. **Copyrights; Trade Secrets:** End User acknowledges and agrees that the structure, sequence and organization of the software (including but not limited to any images, photographs, animations, video, audio, music, and text) are the valuable trade secrets of Intel and its suppliers. End User agrees to hold such trade secrets in confidence. End User further acknowledges and agrees that ownership of, and Intel and its suppliers hold title to, the Product, its copyrights and patents and all subsequent copies thereof regardless of the form or media. End User may not remove from the Product, or alter, any of the trademarks, trade names, logos, patent or copyright notices or making, or add any other notices or marking to the Product.
20. **Governing Law:** The rights and obligations of the parties hereunder shall be construed in accordance with, and all disputes hereunder shall be governed by, the laws of the State of California excluding conflict of law rules and excluding the United Nations Convention on Contracts for the International Sale of Goods. The Superior Court of San Diego County, California and/or the United States District Court for the Southern District of California shall have jurisdiction and venue over all disputes between the parties.
21. **Attorney's Fees And Costs:** In any legal action to enforce this Agreement, or arising out of the sale or licensing of Products hereunder, the prevailing party shall be awarded all court costs and reasonable attorney's fees incurred.
22. **Force Majeure:** Intel shall not be liable to End User for any alleged loss or damage resulting from the delivery of the Products being delayed by acts of End User, acts of civil or military authority, governmental priorities, earthquake, fire, flood, epidemic, quarantine, energy crisis, strike, labor trouble, war, riot, accident, shortage, delays in transportation, or any other causes beyond Intel's reasonable control.
23. **Excusable Delay:** Neither party shall be liable to the other for any alleged loss or a damage resulting from a delay in performance resulting from a cause beyond the reasonable control of the party whose performance is delayed.
24. **Choice Of Language.** The original of this Agreement is in English and End User waives any right to have it written in any other language.
25. **Notices.** Any notice regarding non-performance, breach, termination, or renewal required or permitted to be given under this Agreement shall be given in writing and shall be hand delivered or deposited, postage prepaid, registered or certified mail, in the United States or other country's mail, or sent by express delivery, addressed to End User or Intel, as the case may be, at the addresses stated on the Order or at such other address as shall be given by either one to the other in writing. All other notices may be sent by regular mail or facsimile. All notices shall be deemed given and received on the earlier of actual delivery or three (3) days from the date of postmark.
26. **No Assignment:** End User may not transfer or assign the Product or this Agreement to another party without the prior written consent of Intel.

Glossary

This section defines terms and acronyms used throughout the *Intel® NetStructure™ 7110/7115 e-Commerce Accelerator User Guide.*

Bypass User action causing traffic to bypass 7110/7115 processing, done either through the CLI **bypass** command or Bypass button on the front panel of the 7110/7115.

Cascading A configuration of two or more 7110/7115s serially connected together to accommodate larger e-Commerce traffic processing (CPS) loads.

Certificate A digitally-signed token in an SSL-encrypted transaction containing information including the issuer (Certificate Authority that issued the certificate), the organization that owns the certificate, public key, the validity period for the certificate, and the hostname.

Cipher Any encryption algorithm, either symmetric or public key, operating either as a data stream or divided into blocks.

DNS Domain Name Server. A mechanism used in the Internet for translating the names of host computers into addresses.

Flash Permanent (non-volatile) storage for configuration changes.

Fulfillment Server	A server that stores content used to satisfy user requests.
HTTP	Hypertext Transfer Protocol: the protocol used between a Web browser and a server to request a document and transfer its contents.
HTTPS	HTTP exchanged over an SSL-encrypted session.
Inline	When the 7110/7115 is able to process SSL traffic, the Inline LED on the front panel is lit (blinking or steadily illuminated).
IP	Internet Protocol
IP Address	A unique identifier for a node on an IP network. Expressed in "dotted decimal" notation. For example: 10.0.0.1.
IP Service	A network-accessible, IP-accessible Application Protocol. For example: HTTP, FTP, and the like.
ITM (Internet Traffic Manager)	Intel® NetStructure™ 7140 and 7170 Traffic Director and the Intel® NetStructure™ 7180 e-Commerce Director products used for load balancing.
Key	A public key and private key pair used to encrypt/decrypt messages.
Key Strength	Length, in bits, of keys used in data encryption or authentication. For example: 56, 128, 512.
Keypair	Matching public and private keys.
Load Balancing	The distribution of processing and communications activity across a computer network so that no single device is overwhelmed. Load balancing is particularly important for networks on which it is difficult to predict the volume of requests likely to be issued to a server. Busy Web sites typically employ two or more Web servers in load balancing roles.
Port	In the context of TCP/IP sessions, a unique protocol-specific handle.
Private Key	The part of a key in a public key system that is kept secret and used only by its owner. It is used for decrypting messages and for making digital signatures.
Public Key	The part of a key in a public key system that is distributed widely, and is not kept secure. Used for encryption or for verifying signatures.

Service	A service is an IP application paired with a port number. For example: “HTTP:80.” This describes a service consisting of a server's HTTP application listening on port 80. Another example of a service: “FTP:21.”
Signing Request	Required for a request for certificate authentication by a Certificate Authority.
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol. An application-layer Intenet protocol by which multiple devices in a network can be monitored and to some extent configured.
SSL (Secure Socket Layer)	Protocol developed by Netscape for encrypted transmission over TCP/IP networks, setting up a secure end-to-end link.
VeriSign§	A well-known certificate authority.

Notes

Support Services

Intel offers a range of support services for your new product. You can learn about the options available for your area by visiting the Intel® support Web site at *http://www.intel.com/network/service* and choosing your geography.

Worldwide Access to Technical Support

Intel has technical support centers worldwide. Technicians who speak the local languages staff many of the centers. Visit our Web site at *http://support.intel.com*.

North America only

For support, call **(800) 838-7136** or **(916) 377-7000**.

Japan only

For support, call **+81-298-47-0800**.

Other areas

For support in other countries, use the following table to dial the toll-free support number. Using the table, locate the country from which you are calling, dial the access number, await the dial tone and then dial the listed 800 number.

Country	Dialing Information
Australia	Dial 1-800-881-011, await dial tone, dial 800-838-7136
China [3]	Dial 10811, await dial tone, dial 800-838-7136
Hong Kong	Dial 800-1111, await dial tone, dial 800-838-7136
India [5]	Dial 000-117, await dial tone, dial 800-838-7136

Country	Dialing Information
Indonesia [2]	Dial 001-801-10, await dial tone, dial 800-838-7136
Korea [1]	Dial 0-911, await dial tone, dial 800-838-7136
Malaysia [4]	Dial 800-0011, await dial tone, dial 800-838-7136
New Zealand	Dial 000-911, await dial tone, dial 800-838-7136
Singapore	Dial 800-0111-111, await dial tone, dial 800-838-7136
Sri Lanka	Dial 430-430, await dial tone, dial 800-838-7136
Taiwan [1]	Dial 0080-10288-0, await dial tone, dial 800-838-7136
Thailand [5]	Dial 0019-991-1111, await dial tone, dial 800-838-7136
Austria [1 4]	Dial 022-903-011, await dial tone, dial 800-838-7136
Belgium [1]	Dial 0-800-100-10, await dial tone, dial 800-838-7136
Denmark	Dial 8001-0010, await dial tone, dial 800-838-7136
Finland [1]	Dial 9800-100-10, await dial tone, dial 800-838-7136
France (Includes Andorra)	Dial 19-0011, await dial tone, dial 800-838-7136
Germany	Dial 0130-0010, await dial tone, dial 800-838-7136
Italy (Includes Vatican City) [1]	Dial 172-1011, await dial tone, dial 800-838-7136
Netherlands [1]	Dial 06-022-9111, await dial tone, dial 800-838-7136
Norway	Dial 800-190-11, await dial tone, dial 800-838-7136
Poland [1 3]	Dial 0-0-800-111-1111, await dial tone, dial 800-838-7136
Portugal [3]	Dial 05017-1-288, await dial tone, dial 800-838-7136
Russia [1 2 3]	Dial 755-5042, await dial tone, dial 800-838-7136
Spain	Dial 900-99-00-11, await dial tone, dial 800-838-7136
Sweden	Dial 020-795-611, await dial tone, dial 800-838-7136

Country	Dialing Information
Switzerland [1]	Dial 0-800-550011, await dial tone, dial 800-838-7136
United Kingdom (Mercury) [3]	Dial 0500-89-0011, await dial tone, dial 800-838-7136
United Kingdom (BT) [3]	Dial 0800-89-0011, await dial tone, dial 800-838-7136
RSA (South Africa)	Dial 0-800-99-0123, await dial tone, dial 800-838-7136
Philippines	Dial 105-11, await dial tone, dial 800-838-7136
Vietnam	Dial 12010288, await dial tone, dial 800-838-7136
Pakistan	Dial 0080001001, await dial tone, dial 800-838-7136

Notes:

1	Public phones require coin or deposit
2	Use phones allowing international access
3	May not be available from every phone
4	Public phones require local phone payment through the call duration
5	Not available from public phones

Notes

Index

S

T

U

Notes